WM0824TU Deliverable 2

Group 2

Luca Morgese	**5434033/s2576120**
Fazia Ghuman	**4364554**
Jeffrey Steen	**4641426/s1193074**
Harvey van Veltom	**4350073**
Casper Kroes	**4433882**

1 - Investigate what other actors can influence the security issue

Moving from the metrics individuated in deliverable 1, we propose the following reformulated **security issue (SI)** for Energy distribution systems operators (DSOs): "*Understand the attack volume directed to DSOs relates to cybersecurity properties* [1] *of the country where they operate*".

Researching how cybersecurity in the energy sector is managed, we individuate - besides the single DSO - the main following top-players with respect to the SI:

Regulators (Governments, International Institutions): as energy supply is a critical societal asset, the commitment that local regulators put into promoting cybersecurity determines both incentives and resources for DSOs to implement proper security strategies (TI, controls). Research [1] on the *Global Cybersecurity Index* (GCI) produces a set of per-country metrics that express how regulators can determine the cyber-threat preparedness environment for the industries they host. National and international intelligence agencies may further cooperate to the benefit of such an environment [2] and national strategies can be outlined towards the same goal, contributing to the SI (as in [3]).

TI market actors: TI agencies can play a core role in informing (Energy) Companies' awareness of the threat environment [4]. Their role in the security issue can thus be directly observed: where multiple private TI providers compete in the same market, it is natural for the contribution of such TI services to the SI to be higher, both in the sense of the quality of the provided information and in their involvement to the overall cyber-threat preparedness of a country [5].

Third-party DSOs: peer cooperation to tackle cyber-threats can produce highly valuable TI among same-industry actors (shared TI, [4]). Where multiple DSOs can join a united strategic cybersecurity front, an evident and direct impact on the SI is observed [6], [7]. The incentive for such consortia is very high, as such organizations represent a natural, sound, and obvious response to the evolving threat environment [8].

Cybersecurity researchers: concerns OTI sources and autonomous researchers in the area of TI and cybersecurity. Of course, those sources shall contribute to the SI where they make resources available to improve the cyber-threat preparedness of any institution.

Below, a power-interest grid frames the above actors with respect to the security issue.

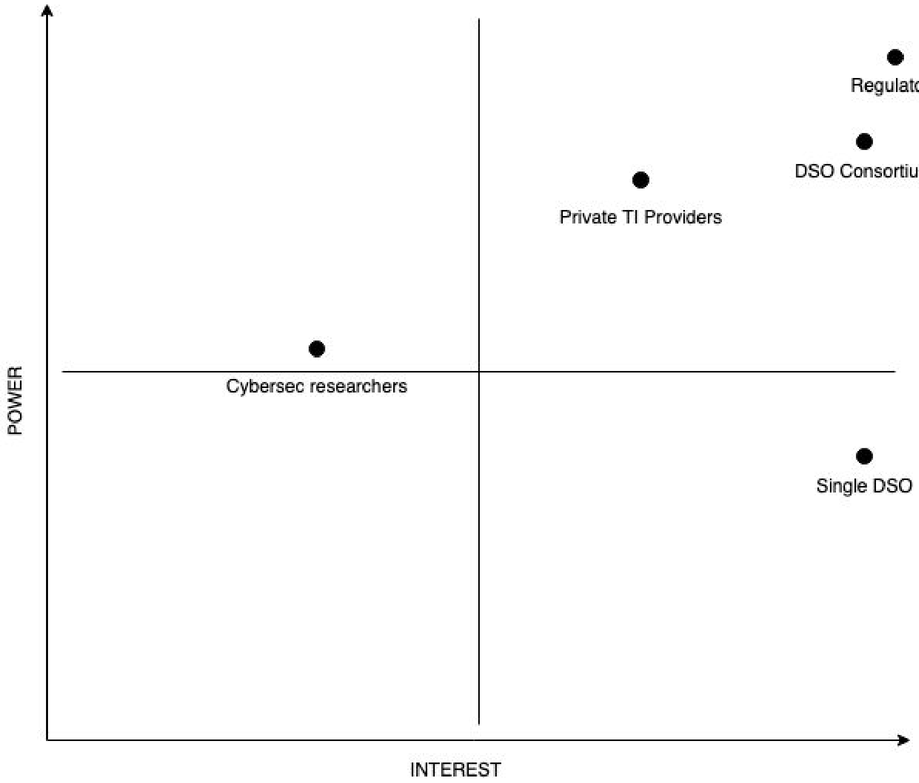


Table 1: power-interest grid between actors and the SI.

2 - Identify the risk strategies that these actors can adopt to tackle the problem (1 point)

a. **Are there actors with different strategies? Why?**
b. **Have the strategies changed significantly over time in a way that reduces or increases risks?**

Regulators. As the most powerful and interested entities [3], [9], regulators shall design the digital environment preparedness to address the security issue. A risk-strategy may consist of: a. constitute dedicated panels to perform state-level risk assessments of Energy grid capabilities, involving DSO and State representatives, and cybersecurity experts; b. build a normative framework or plan to support and incentivize cybersecurity and resilience of energy grid assets; c. constitute dedicated intelligence boards; d. aim at long-term, flexible and strong measures, considering the shape of the threat landscape and the criticality of Energy assets [7], [10].

TI Market Actors. It is inherent in the business model of private TI providers to tackle the SI for all client companies with digital assets. As [5] reports, as key holders of TI, they may contribute to Public Sector panels to address the overall status of a Country's preparedness against digital threats. With this respect, proper incentives have to be put in place by Regulators.

Third-party DSOs. As encouraged by Regulators' plans [11] and prompted in various initiatives [12], [6], a viable and valuable risk strategy that the whole network of DSOs can undertake concerns forming a united cybersecurity front, meaning: a. setup standards and capabilities to collect TI on own infrastructure [12]; b. implement TI sharing protocols among members of DSO consortium; c. design plans to offer strategic redeployment of energy or cybersecurity capabilities in case of need; d. constantly assess and define the evolving threat environment to better strategize. Incentivization should come naturally among DSO towards such a strategy, considering the evolution of digital energy grids - which brings interconnection and extended attack surface - and of cyber threats [10].

Cybersecurity Researchers. Again under proper incentivization by DSOs and/or Regulators, cybersecurity researchers shall inherently aim at improving the state of art concerning threat detection and prevention, focusing on standardization and scalability to ease information sharing. Naturally, as new technologies are available to the public or private domain, stronger controls can be put in place by DSOs against cyber-threats.

a. Actors have different risk management strategies, as they approach the SI from different sides: Regulators have direct policy-making power and interest in protecting the integrity of local energy grids; private market players respond to the SI with services built with a primary for-profit interest; partner DSOs concur to a single cybersecurity front to enforce the most efficient, sector-specific and direct approach to counter cyber threats.

b. Rather than changed, strategies had recently evolved because of the relative new design of digital-backed power grids. Risks raise as digital inter-connection and e-governance take hold, and cyber-threats become more powerful and organized [6]. Attack surfaces become greater, attackers become smarter, energy remains a critical societal asset. The necessity arises for cohesive efforts and effective risk management strategies that have to be devised by the multitude of involved actors (notes on incentives). "Lonely hero" approaches to cybersecurity are doomed to fail against new APTs, and stakeholders need to promote standardization to unify the cybersecurity front [7].

3 - Select 3 actors (including the problem owner) involved in the security issue (you can draw on the previous assignment). For each one:

a. **(0.5 point) Identify one concrete countermeasure that they could take to mitigate the security issue,**
b. **(0.5 point) Analyse the distribution of costs and benefits (without quantifying) among the different actors that the deployment of the countermeasure would entail,**
c. **(1 point) Analyse whether the actors have an incentive to take the countermeasure,**
d. **(1 point) Briefly reflect on the role of externalities around this security issue.**

DSO (problem owner)

a) *Implementing a communication channel with State representatives and State intelligence services* is a countermeasure that would directly address the SI. As each of the two parties share respective TI knowledge and dynamic assets requisites, cybersecurity policy-making on both sides is naturally improved [12].
b) DSO costs would consist of opening a (small) dedicated department for - or integrating procedures to implement - such communication channel. Involved regulators would have to select representatives. Both would have to produce reports to share knowledge and needs, as well as processing both. Resulting costs would be but primarily timely and organizational, possibly negligible, if considered that both parties would benefit from an ad-hoc TI sharing channel to protect Energy-related assets: improved security posture for DSOs, improved awareness, and control-power for regulators.
c) As above explained, regulators and DSOs both would have a natural incentive to implement a similar measure, the first to protect the business, the second to implement good governance.
d) Double-side externalities would arise: as more DSOs implement this measure, the centralized TI sharing model $(DSO_i \leftrightarrow Regulator)$ allows the Regulator to gather direct TE insights from the whole sector, and redistribute such knowledge to each DSO. Regulators are more informed and improve State security policy-making and posture, DSOs receive higher quality TI.

Regulators:

a) *Establishing a panel to investigate (cyber)security of the Country's Energy assets* is a viable measure that would contribute to an actual State cybersecurity strategy, directly addressing the SI [9]. The panel would model the cyber-profile of the Energy network and produce high-level risk-assessment reports to frame a cybersecurity preparedness, determining critical assets and needs, formulating recovery plans. This countermeasure could be integrated with the one individuated for DSOs.
b) Costs would be related to building and managing such task-force in terms of budget, timings, and resources, and the direct benefit of such "countermeasure" is self-manifest for Regulators, and concerns improving governance: strengthening the security and continuity of the nation's Energy supply - eventually gaining strategic advantages over less-prepared countries - and generate a consistent view of cybersecurity posture in the Energy sector, to align stakeholders. Direct DSOs involvement is not necessarily required, but it is obvious that they would benefit from the investigations of such panel, similarly as in the preceding example.
c) A measure as "simple" as setting up such a panel could bring about a new level of awareness in the State-level cyber threats landscape for specific sectors (Energy, in our case). Besides, higher regulator's commitment to cybersecurity would naturally render the State more attractive to DSOs (and other companies) - which could access TI resources more easily - overall leading to a more thriving market and improved services. The incentive to a similar measure is thus inherent with the activity of regulators.
d) Externalities related to this countermeasure and the SI could indeed concern DSOs being interested in taking part in a Country-level cybersecurity strategy, to take advantage of and improve the State-produced TI. Private TI providers could have to

align with the scenario via either improving, differentiating, or integrating their services in the process. Overall, a higher understanding of the TE by all stakeholders shall be reached.

Third-party DSOs

a) *Setting up a consortium for TI and cybersecurity cooperation* would allow DSOs to have a better understanding of both what attacks they are facing, as well as obtain further insights on the characteristics of DSOs in a country that attracts or deters attackers. This would be more potent if the consortium contained DSOs from several countries, for comparison.

b) There will be a need for an organisation that manages the sharing of information and strategy. The costs for such an organization can be amortised over the consortium members. Sharing TI information could reduce the competitive advantages certain DSOs have over others. Due to having information about other DSOs, and which attacks they are facing, DSOs can gain a better understanding of what makes them more or less attractive to attackers. Overall though, as DSOs make a more unified and informed effort to protect against cyberattacks, the whole energy grid would be less likely to be victim of cyber-threats [13].

c) Having more information about the threat landscape, and which strategies other DSOs are employing, and to which effectiveness, will allow participating DSOs to better protect themselves against attacks. For this reason, they are incentivised to participate in the consortium. DSOs that do not join the consortium will likely have a weaker defense against attacks, making them more attractive targets. DSOs within the consortium will eventually lose cybersecurity-related competitive advantages over each other but will gain competitive advantages over DSOs, not in the consortium. This makes the consortium most attractive to DSOs with weak cybersecurity. Additionally, DSOs may want to join the consortium to compare their cybersecurity performance with other DSOs. Research has shown that companies, when shown their performance are below the industry standard, will invest more in cybersecurity, and increase their performance. [14]

d) A direct benefit comes from direct network effect. As more Energy companies join the consortium, the total amount of information to improve TI awareness and setup readiness will increase, attracting more DSOs to join the consortium.

4. Statistical analysis

4.1 Metric and actor choice

For this assignment we took the frequency of Indicator of Compromise tags per country as a metric, and refined it further by normalising it by dividing it by the overall amount of Indicators of Compromise (across all sectors) tagged with a specific country:

$$Rel.IOC\ frequency_{country} = \frac{\Sigma IOC_{energy}}{\Sigma IOC_{allSectors}}$$

This is done because if there is a bias resulting in certain countries being overrepresented in the OTX this should be the case for all sectors. The resulting metric is the relative IOC volume targeting the energy sector. The primary actor that influences this metric is the national government of the country. The national government often has a monopoly on the corporations in charge of the energy infrastructure [15] and therefore can be seen as a single actor responsible per country.

4.2 Factors explaining possible variance

Many factors can explain variance in IOC volume ([16]–[18]) but finding quantitative data for these factors is challenging. In this case, two factors were used: the GCI, and the overall energy production as provided by the IEA. The overall energy production is used as a proxy for the potential effect size that an attack could have.

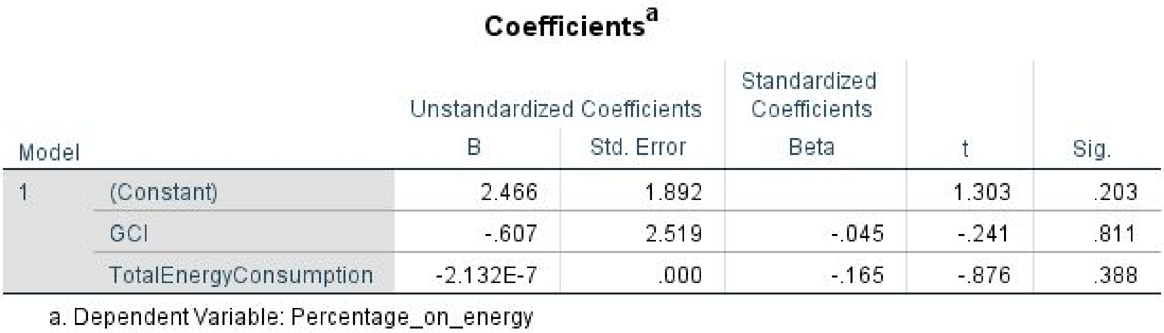
Factor	Source in literature for relation	Source for data
GCI	[1]	https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
Effect size (i.e. potential damage done)	[16]	https://www.iea.org/data-and-statistics?country=WORLD&fuel=Energy%20supply&indicator=TPESbySource

Table 2: factors explaining variance in relative IOC volume

4.3 Method

All countries within the OTX that have more than 100 IOCs related to the energy industry were used (total of 37 countries). There were 2 big outliers in the resulting dataset: the UAE with a relative volume of 23% and Azerbaijan with 14%. These were removed. The other countries had volumes between 0 and 8%. The data also has some weird characteristics because countries that had attacks on their Energy infrastructure that made international headlines such as Ukraine and the United States score relatively low. This raises some questions regarding the completeness of the data and whether Alienvault contains enough data to be representative of the threat landscape. The absolute amount of IOCs regarding the energy sector was also added, and this was combined with the GCI and Total Annual Energy Production of the remaining countries. After this, a regression analysis was done to check if there is any (linear) relation between the GCI and Total Energy production and the relative IOC frequency.

4.4 Results:



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	2.466	1.892		1.303	.203
	GCI	-.607	2.519	-.045	-.241	.811
	TotalEnergyConsumption	-2.132E-7	.000	-.165	-.876	.388

a. Dependent Variable: Percentage_on_energy

Table 3: Regression analysis result

Regrettably, the results of the regression analysis are not significant (as Sig > 0.05), meaning that within our data set there is no measurable linear relation between the relative IOC volume and a countries' GCI or total energy consumption. This could mean that attackers use other characteristics to pick their targets. That said, additional research combining more data sources is necessary to make any definitive claims about this. The Total Energy Production and the Total Number of IOCs related to a country do correlate, although this is to be expected since it is to be expected that both these indicators correlate with a countries size.

Bibliography

[1] ITU, ‘Global Cybersecurity Index 2018’. 2019, Accessed: Oct. 05, 2020. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[2] ‘BT joins forces with Europol to build a safer cyber space’, *Europol*, May 15, 2018. https://www.europol.europa.eu/newsroom/news/bt-joins-forces-europol-to-build-safer-cyber-space (accessed Oct. 10, 2020).

[3] ‘National Cybersecurity Strategies’, *ENISA*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies (accessed Oct. 05, 2020).

[4] X. Bouwman, H. Griffioen, J. Egbers, C. Doerr, B. Klievink, and M. van Eeten, ‘A different cup of TI? The added value of commercial threat intelligence’, 2020, pp. 433–450, Accessed: Sep. 17, 2020. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/bouwman.

[5] B. Farrand and H. Carrapico, ‘Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism’, in *Security Privatization*, O. Bures and H. Carrapico, Eds. Cham: Springer International Publishing, 2018, pp. 197–217.

[6] ‘Energy Sector Cybersecurity Preparedness’, *Energy.gov*. https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity (accessed Oct. 05, 2020).

[7] N. Richet, ‘Cybersecurity implications of the Energy sector evolutions’, presented at the E.DSO ENCS ENTSO-E Workshop, Oct. 07, 2020, [Online]. Available: https://www.edsoforsmartgrids.eu/e-dso-encs-entso-e-workshop-cybersecurity-data-sharing/.

[8] EECSP, ‘New report on Cyber Security in the Energy Sector published’, *Energy - European Commission*, Mar. 03, 2017. https://ec.europa.eu/energy/news/new-report-cyber-security-energy-sector-published_en (accessed Oct. 05, 2020).

[9] D. Healey, S. Meckler, U. Antia, and E. Cottle, ‘Cyber Security Strategy for the Energy Sector’, European Parliament, Directorate General for Internal Policies, Oct. 2016. [Online]. Available: http://publications.europa.eu/resource/cellar/8cf0f709-fcb9-11e6-8a35-01aa75ed71a1.0001.01/DOC_1.

[10] F. Strempfl, ‘System Operators & Market Enabler Network Code on Cybersecurity and Data Sharing’, presented at the E.DSO ENCS ENTSO-E Workshop, Oct. 07, 2020, [Online]. Available: https://www.edsoforsmartgrids.eu/e-dso-encs-entso-e-workshop-cybersecurity-data-sharing/.

[11] Energy.gov, ‘The U.S.-Israel Energy Center Announces Funding Opportunity for Energy Infrastructure Cybersecurity Cooperation’, *Energy.gov*. https://www.energy.gov/articles/us-israel-energy-center-announces-funding-opportunity-energy-infrastructure-cybersecurity (accessed Oct. 12, 2020).

[12] S. Kadhi, ‘SHARING IS (S)CARING STRATEGIES FOR COMBATTING CYBERATTACKS’, presented at the E.DSO ENCS ENTSO-E Workshop, Oct. 07, 2020, [Online]. Available: https://www.edsoforsmartgrids.eu/e-dso-encs-entso-e-workshop-cybersecurity-data-sharing/.

[13] F. Fransen, A. Smulders, and R. Kerkdijk, ‘Cyber security information exchange to gain

insight into the effects of cyber threats and incidents’, *E Elektrotechnik Informationstechnik*, vol. 132, no. 2, pp. 106–112, Mar. 2015, doi: 10.1007/s00502-015-0289-2.

[14] M. van Eeten and H. Asghari, ‘THE ROLE OF INTERNET SERVICE PROVIDERS IN BOTNET MITIGATION: AN EMPIRICAL ANALYSIS BASED ON SPAM DATA STI WORKING PAPER 2010/5’, p. 67, 2010.

[15] J.-M. Glachant, M. Saguan, V. Rious, and S. Douguet, *Incentives for investments : comparing EU electricity TSO regulatory regimes*. 2013.

[16] M. B. Line, A. Zand, G. Stringhini, and R. Kemmerer, ‘Targeted attacks against industrial control systems: Is the power industry prepared?’, in *Proceedings of the 2nd Workshop on Smart Energy Grid Security*, 2014, pp. 13–22.

[17] K. Vasileiou, ‘Cybersecurity in the energy sector: a holistic approach’, Master’s Thesis, University of Piraeus, 2019.

[18] A. C. Sharma, R. A. Gandhi, W. Mahoney, W. Sousan, and Q. Zhu, ‘Building a social dimensional threat model from current and historic events of cyber attacks’, in *2010 IEEE Second International Conference on Social Computing*, 2010, pp. 981–986.

Task division

Casper Kroes: Analysis for question 4 including refining the Python code.
Luca Morgese: outlined and contributed to points 1, 2 and 3 with related research.
Fazia Ghuman: Contributed to 4, general literature research for overall refinement.
Jeffrey Steen: Contributed to 1 and 3, literature research, proofreading.
Harvey van Veltom: General proofreading of sections 1-3, proofreading, and contributed to section 4.