frontiers in Computer Science

ORIGINAL RESEARCH
published: 10 March 2021
doi: 10.3389/fcomp.2021.614337

Cyber Hygiene Maturity Assessment Framework for Smart Grid Scenarios

Inna Skarga-Bandurova[1,2]*, *Igor Kotsiuba*[2] *and Erkuden Rios Velasco*[3]

[1]*Visual Artificial Intelligence Laboratory, School of Engineering, Computing and Mathematics, Oxford Brookes University, Oxford, United Kingdom,* [2]*Digital Forensics Research Laboratory, Department of Mathematical and Econometric Modeling, Pukhov Institute for Modelling in Energy Engineering, Kyiv, Ukraine,* [3]*TECNALIA, Basque Research and Technology Alliance (BRTA), Derio, Spain*

Cyber hygiene is a relatively new paradigm premised on the idea that organizations and stakeholders are able to achieve additional robustness and overall cybersecurity strength by implementing and following sound security practices. It is a preventive approach entailing high organizational culture and education for information cybersecurity to enhance resilience and protect sensitive data. In an attempt to achieve high resilience of Smart Grids against negative impacts caused by different types of common, predictable but also uncommon, unexpected, and uncertain threats and keep entities safe, the Secure and PrivatE smArt gRid (SPEAR) Horizon 2020 project has created an organization-wide cyber hygiene policy and developed a Cyber Hygiene Maturity assessment Framework (CHMF). This article presents the assessment framework for evaluating Cyber Hygiene Level (CHL) in relation to the Smart Grids. Complementary to the SPEAR Cyber Hygiene Maturity Model (CHMM), we propose a self-assessment methodology based on a questionnaire for Smart Grid cyber hygiene practices evaluation. The result of the assessment can be used as a cyber-health check to define countermeasures and to reapprove cyber hygiene rules and security standards and specifications adopted by the Smart Grid operator organization. The proposed methodology is one example of a resilient approach to cybersecurity. It can be applied for the assessment of the CHL of Smart Grids operating organizations with respect to a number of recommended good practices in cyber hygiene.

Keywords: cyber hygiene, resilience, critical infrastructure, smart grid, maturity assessment, framework

OPEN ACCESS

Edited by:
Fabrizio Baiardi,
University of Pisa, Italy

Reviewed by:
Gabriele Costa,
IMT School for Advanced Studies Lucca, Italy
Damián López,
Universitat Politècnica de València, Spain

***Correspondence:**
Inna Skarga-Bandurova
iskarga-bandurova@brookes.ac.uk

Specialty section:
This article was submitted to Computer Security, a section of the journal Frontiers in Computer Science

Received: *05 October 2020*
Accepted: *18 January 2021*
Published: *10 March 2021*

Citation:
Skarga-Bandurova I, Kotsiuba I and Velasco ER (2021) Cyber Hygiene Maturity Assessment Framework for Smart Grid Scenarios. Front. Comput. Sci. 3:614337. doi: 10.3389/fcomp.2021.614337

INTRODUCTION

The growth of Smart Grids is causing a complex transformation of electricity generation and distribution into new flexible integrated transmission and distribution systems. The idea of innovative transformation of the power industry involves the development and implementation of distributed, self-regulating energy systems, which include generating sources and backbone and separate networks where all types of consumers are served by the intelligent network in real time. Unlike traditional solutions designed to transport electricity from a generator set to end-users through a unidirectional flow of power and a centralized control system, modern Smart Grids are fully distributed systems that make extensive use of computer remote control and automation. Peculiarities of the organization of intelligent distributed electricity networks pose risks associated with their implementation, operation, and modernization. Compared to traditional power systems, the Smart Grid merges the multiply technologies into the dynamic and interactive infrastructure,

which provide full integration of millions of power devices and sensors, enabling prompt bilateral energy transmission, monitoring, and energy management through the advanced communications system and smart meters, such as Advanced Metering Infrastructure (AMI), directional relays (DR), and demand-side management (DSM) (Wang and Lu, 2013). At the same time, intensive information exchange makes the Smart Grids vulnerable to a number of malicious threats related to telecommunications and network systems. This jeopardizes the reliable and safe operation and is touted as the key objective of the Smart Grid. Intruders can lead to a number of serious consequences in the network, which can lead to the disclosure of private information, disruptions, power outages, or even the destruction of infrastructure. Thus, along with other features of the Smart Grid, cybersecurity and resilience are becoming critical issues, as a number of electronic devices are interconnected through information communication networks at critical facilities that directly affect the reliability of such a vast infrastructure. As the energy system is one of the main key public infrastructures, damage to any component of the network can lead to huge losses in terms of the country's economy and social welfare.

There are two related but different approaches for understanding system response to changes; they are vulnerability and resilience (Miller et al., 2010). As mentioned by Linkov et al. (Linkov et al., 2019), "resilience as a philosophy and methodology seeks to better prepare complex systems for a variety of threats," whereas "vulnerability is seen as a condition, encompassing characteristics of exposure,... shaped by dynamic processes and power relations..." (Blaikie et al., 1994; Downing et al., 2005; Eakin and Luers, 2006).

According to Saed et al. (Saed et al., 2013), there are four main classes of vulnerabilities that create significant risks and open the possibility of various cyberattacks as follows. 1) People, policy, and procedure, lack of necessary training and noncompliance with policies and procedures cause numerous security risks and issues. 2) Vulnerabilities in software and firmware: it sounds reasonable when stakeholders need certain access permission to the system in accordance with their technical responsibilities. The system software and unsigned firmware are susceptible to different types of attacks and can be compromised by hackers. 3) Platform vulnerabilities: exacerbating the problem is that each smart device could be delivered with its own firmware; this means that several vulnerabilities could appear on a single device. 4) Network service vulnerabilities: particular issues associated with system architecture and configuration can result in a situation where the operating system and hardware have a common network security problem. Traditionally, networks suffer from weakness in hardware, software, or organizational processes and involve data, software, or physical assets.

People are both a major asset and a major business vulnerability. It is a matter of common knowledge that the top tier attacks employ common security breaches and the success of cyberattacks is entirely dependent on the cyber habits within the target organizations. For example, one of the problems posed by attacks targeting smart meters or sensors and actuators to monitor and control some physical process is that most users are not even aware of the computational nature of smart objects. The awareness of the computational powers of smart objects and even of the objects themselves disappears as they become more pervasive and diffused (Greenland Energy Profile, 2018). With that in mind, the training and awareness programs targeted on good practices in cybersecurity and cyber hygiene for every Smart Grid user (in electricity organizations or in smart home) are vital. To reduce the chances of becoming a victim or spreading an attack, people need to be educated about cybersecurity best practices pertinent to domestic and professional situations and should be able to put in force cyber hygiene rules.

Cyber hygiene (CH) is the core concept of training organizations to be proactive about cybersecurity in order to offset the risk of cyber threats and security issues (Norton, 2020). The Center for Internet Security (Energy statistics, 2017) defines CH as a set of baseline cybersecurity protective activities that help implement security in an organization. The CH is defined as a set of protection procedures, policies, and rules to address cyber risks in Smart Grids. This is a preventive approach to security. We devise the cyber hygiene framework as recommendations and training materials. The framework will enclose a list of potential cyber threats in terms of confidentiality, integrity, and data availability. The main purposes of CHMF creation are as follows: (i) to incorporate cyber hygiene practices for utility services and operations where they have not been used before, e.g., personnel training, network segregation, device, and network passwords; (ii) to enable continuous and periodic assessment in use case scenarios such as substation operator, smart home user, and hydropower plant; (iii) to find a broader knowledge of how and when hygiene techniques could be useful against common cyber threats. The CHL measurement will reveal current cyber awareness maturity among personnel and will allow organizations to provide a tailored set of cyber hygiene training for users and management. This approach should help educate the end-users on SPEAR tools and their functions, as well as increasing concern and commitment to the Smart Grid cybersecurity protection.

MATERIALS AND METHODS

Standards

There are a set of standards related to Smart Grid CH. A good point to computing a Cyber Hygiene Level (CHL) regarding several cybersecurity standards includes ISO/IEC 27001 & 27002, ISO/IEC 27001:2013 "Information technology—Security techniques—Information security management systems—Requirements," and ISO/IEC 62351 "Security Standard for TC 57 series of protocols." Other NIST& NERC cybersecurity references include the following: NIST Special Publication (SP) 800-53 Rev.4 "Security and Privacy Controls for Federal Information Systems and Organizations," NIST SP 800-82 Rev.2 "Guide to Industrial Control Systems (ICS) Security," NIST SP 800-63-2 "Electronic Authentication Guideline," NIST SP 800-57 Part 1 Rev.4 "Recommendation

for Key Management," NIST CAVP (2018)-Cryptographic Algorithm Validation Program, NIST CMVP-Cryptographic Module Validation Program based on FIPS 140-2 requirements, NIST SP 800-52 Rev.1 "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations," NIST SP 800-81 Rev.2 "Secure Domain Name System (DNS) Deployment Guide," NIST SP 800-77 Guide to IPSec VPNs, NIST SP 800-113 "Guide to SSL VPNs," NIST SP 800-88 Rev.1 "Guidelines for Media Sanitization," and NERC CIP v5 "Critical Infrastructure Protection" standard framework.

EU Projects and Initiatives

As mentioned in Inria White Book No. 3 (2019), there are several EU initiatives promoting the CH path. The French Agence Nationale de la Sécurité des Systèmes d'Information (2013) (ANSSI) put together the "40 Essential Measures for a Healthy Network" in a guide for people responsible for the security of information systems. The ENISA issued a set of CH practices (ENISA Europa EU, 2017b, Cyber Hygiene). The ECSO developed the "Cybersecurity Human Resources Network" aimed at increasing awareness about various CH initiatives (ECS, 2018, WG5). Besides, there are a number of EU initiatives that do not focus on CH but address challenges for Smart Grid cybersecurity and suggest high-level technological solutions. For example, there are several EU-funded projects working on this topic as follows: The Community Research and Development Information Service (CORDIS, 2020) of the European Commission returns 1,018 results for the queries related to the "Smart Grid," 239 results for "Smart Grid security,-" and 4 results for query "cyber hygiene." After a detailed analysis, we summarize below the following seven projects: SPARKS, UMBRELLA, SEGRID, SUCCESS, DRIM-GO, SIPSEC, and PROTECTIVE.

SPARKS, Smart Grid Protection Against Cyber Attacks project (2014–2017), https://project-sparks.eu/, provides several innovative Smart Grid security solutions with application to risk assessment, development of reference architectures for secure Smart Grids, and suggestions on Smart Grid security standards. Several novel techniques based on big data for security analytics in Smart Grids and hardware tools for smart meter authentication are investigated. The project identifies the specific challenges associated with Smart Grid cybersecurity risk assessment that provides a deeper understanding of cyber-physical nature and risks related to the interconnection between legacy systems and Smart Grid systems. Although the cyber hygiene politics and approaches are out of the scope of this project, there are some results relevant to this topic. For example, in the publication on Social Engineering Attacks and the Smart Grid (The SPARKS Project, 2015), it was outlined that many organizations are focused on education as the core component of user awareness in the area of social engineering attacks. It was also noted that "analytics-based approach" or "intelligence-driven security" should be adopted by organizations to respond to such attacks.

UMBRELLA, Toolbox for Common Forecasting, Risk assessment, and Operational Optimization in Grid Security Cooperations project (2012–2015) FP7-ENERGY—Specific Program "Cooperation": Energy, is targeted toward the development of the toolbox that enables Transmission System Operators (TSOs) to ensure secure grid operation and innovative power flow management in future electricity systems with substantial contributions from intermittent renewable energy sources (RESs). The UMBRELLA team delivered a set of recommendations for relevant stakeholders. These proposals help enhance interoperability and security in the pan-European grid system and enable data exchange so that developed software tools can be applied by TSOs and within Regional Security Cooperation Initiatives (RSCIs).

SEGRID, Security for smart Electricity GRIDs project (2014–2017) FP7-ENERGY—Specific Program "Cooperation": Energy, was targeted toward defending Smart Grids against cyberattacks through six actions: 1) threats identification; 2) security standards gap analysis for Smart Grids; 3) development of new security approaches for ensuring privacy and Smart Grids system security; 4) elaboration of Security Integration Test Environment (SITE) to test and verify the new security approaches; 5) evaluation and improvement of risk management methodologies in terms of tailoring them to the Smart Grids; 6) implementing obtained results into European standardization bodies and Smart Grid industrial providers.

SUCCESS, SecUring CritiCal Energy infraStructureS project (2016–2018), https://www.success-energy.eu/, aimed at developing a comprehensive approach to threat analysis with special focus on the Smart Meters (SM) vulnerabilities. Being one of the core components of Smart Grid, SM need to be considered from a security requirement perspective. For this purpose, SUCCESS developed a set of concrete guidelines to support the design of energy systems and their linked communications networks.

DREAM-GO, enabling Demand Response for short and real-time Efficient And Market based smart Grid Operation project (2015–2019), http://dream-go.ipp.pt/, is targeted toward the Smart Grids consumption flexibility and positioning the consumer as an active player. The central role of the consumer in this project enables developing and implementing a set of consumer remuneration strategies allowing the key players to interact with each other.

CIPSEC, enhancing Critical Infrastructure Protection with innovative SECurity framework project (2016–2019), https://www.cipsec.eu/, developed a unified security framework and ecosystem for cybersecurity protection of critical infrastructure (CI) in particular at IT (information technology) and OT (operational technology) departments. The project offered a set of additional services such as forensics analysis of public-private partnerships, vulnerability tests, security recommendations, standardization and protection against cascading effects, and training courses for the CI key personnel.

PROTECTIVE, Proactive Risk Management through Improved Cyber Situational Awareness project (2016–2019), https://protective-h2020.eu/, developed a comprehensive solution to raise organizational cyber situational awareness. It is performed by enhancing security alert correlation and prioritization, linking the relevance/criticality of an organization's assets to its business/mission, and establishing a TI sharing community.

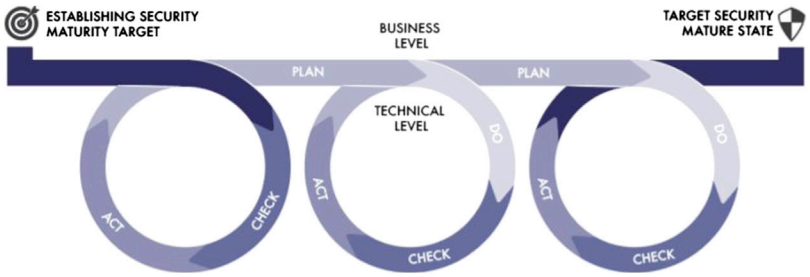

FIGURE 1 | SMM improvement cycle (ENISA, cyber hygiene).

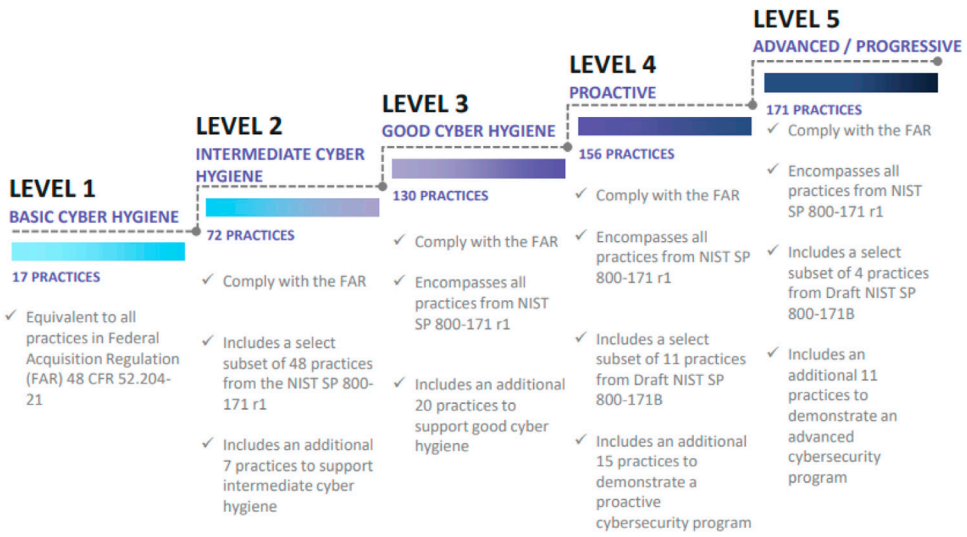

FIGURE 2 | CMMC maturity process progression (CMMC, 2020).

Cybersecurity and Cyber Hygiene Maturity Models

Cybersecurity maturity model certification is a trend that is going on, followed by industrial enterprises, that enables bolstering security through enhanced visibility and improved defending practices.

The Internet of Things Security Maturity Model: The Industrial Internet Consortium®

The Industrial Internet Consortium® (IIC™) proposes a Security Maturity Model (SMM) for the IoT providers, providing them with a roadmap to gain a certain level of security according to the requirements and eliminating overinvesting in unnecessary security mechanisms (Bertino and Islam, 2017; Industrial Internet Consortium, 2018). As mentioned in the (ENISA Europa EU, 2017b, Cyber Hygiene) report, "the maturity model is based on the Plan-Do-Check-Act (P-D-C-A) cycle (Act, in this case, means accepting a new baseline if the check on the result of the improvement step is successful)." The P-D-C-A cycle begins by establishing the security maturity goal for the targeting system. The next steps involve an iterative process directed on the improvement of the security maturity, as shown in **Figure 1** (ENISA Europa EU, 2017b, Cyber Hygiene).

Cybersecurity Maturity Model Certification by NIST SP 800-171

The CMMC (Cybersecurity Maturity Model Certification, 2020) is a unified cybersecurity standard for future DoD acquisitions. We include cybersecurity maturity model certification in this review since it is one of the essential tools that the United States Government applies to audit contractor compliance with NIST SP 800-171. This procedure shows the level of adoption of the standards and indicates the set of requirements an organization faces throughout all levels from Level 1 up to Level 5 (**Figure 2**). The CMMC framework lists the most common practices and processes mapped through 17 maturity capability domains.

The following standards are mapped in the CMMC: ISO 27002, NIST Cybersecurity Framework (2020), NIST 800-171 rev2, NIST 800-171B, NIST 800-53 rev4, FAR 52.204-21, CERT RMM v1.2, CIS (2019) Critical Security Controls v7.1, and Secure Controls Framework (SCF) and other control frameworks.

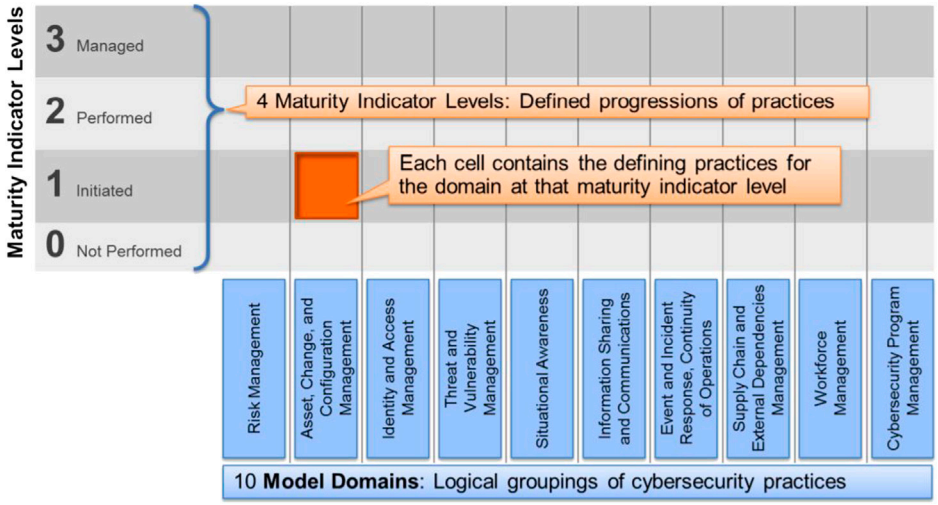

FIGURE 3 | C2M2 for IT services model architecture (C2M2, v1.0, 2015).

Awareness & Training Maturity Capability (AT-MC) includes CERT RMM v1.2 and SCF: (i) establish a policy that includes Awareness & Training (AT); (ii) document the CMMC practices needed to apply the AT policy; (iii) setup, realize, and supply the AT plan; (iv) inspect and measure the efficiency of AT activities; (v) standardize and optimize a documented approach for AT within all organization.

The AT must include CERT RMM v1.2, CIS v7.1, NIST 800-53 rev4, NIST 800-171 rev2, ISO 27002, NIST CSF, and SCF: (i) ensure that all those concerned (managers, system administrators, and end-users) are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems; (ii) produce *ad hoc* security training on how to recognize the insider threats and how to report them; (iii) provide awareness training focused on how to recognize and respond to the social engineering incidents, security breaches, different types of suspicious behaviors, and advanced persistent threat actors; (iv) have practical exercises in cybersecurity awareness training tailored to the current threat scenarios; (v) evaluate the level of awareness of personnel to be sure that people are able to carry out assigned information security-related duties and responsibilities.

Cybersecurity Maturity Model Certification by SEI

The CMMC for Information Technology Services (C2M2 for IT Services, 2015) by the Software Engineering Institute (SEI) is developed based on the Cybersecurity Capability Maturity Model (C2M2, U.S. Department of Energy, 2014a; U.S. Department of Energy, 2014b) and the Electricity Subsector C2M2 (ES-C2M2, 2014). The model enables evaluating the level of adoption of cybersecurity practices on typical enterprise IT services. Organizations can use C2M2 as a self-evaluation methodology to measure their cybersecurity program and improve it. The model covers 10 domains (see **Figure 3**). Each domain includes a set of cybersecurity practices grouped by objective, e.g., risk management, threat and vulnerability management, and configuration management. These practices are ordered within each objective and vary by maturity indicator level (MIL) (CMMC, v01, 2020).

The newest version of the model (Cybersecurity Capability Maturity Model Version 2.0, June 2019) suggests four maturity levels from MIL0, where practices are not performed, to MIL3, where objectives and practices are established and monitored.

Summary on Standards and Best Practices

As mentioned in ENISA's review of CH practices (ENISA Europa EU, 2017b, Cyber Hygiene), to this moment, every EU Member State has its own CH programs or guidance. Most of these programs are aligned with, or driven by, the National Cyber Security Strategies (ENISA Europa EU, 2017a, National Cybersecurity Strategies—Interactive Map) and are at varying levels of maturity. Some of the predominant ones are the Belgian Cybersecurity guide, which also provides an assessment questionnaire for businesses, the "40 Essential Measures for a Healthy Network" report produced by ANSSI and the "Cyber Essentials Guidance" of the United Kingdom government. Furthermore, the approval of the European NIS Directive and the creation of the Cybersecurity Competence Center Network in Europe are paving the way toward a homogeneous CH strategy across Europe.

Summarizing existing general CH modules and education, our analysis revealed that most of the previous projects tend to raise organizational cyber situational awareness in Smart Grids; many of them have contributed heavily in cybersecurity while comprehensive strategy and methodological approach for evaluating CH maturity level have not been developed yet. There are several European initiatives targeted at producing CH frameworks on a wide-scale basis. For stepping up the practical activities to this end and making them more specific to the energy sector, electricity and Smart Grids equipment is badly needed. As a result, we conclude that, aside from the cybersecurity tools development, it is necessary to promote a

holistic approach to CH management with the ultimate goal of cultivating a strong cybersecurity culture in Smart Grids and best practices adoption. The CH management shall be pivoted by (i) CHMM to enable the assessment of the cybersecurity posture of the organization; (ii) increasing training dynamics and awareness methods for Smart Grid cybersecurity; (iii) continuous enhancing cybersecurity skills.

The growing complexity of the Smart Grid infrastructure, their security components and tools used for cyberattack detection, mitigation, and information sharing such as Security Incident and Event Management (SIEM) systems, AMI Honeypots, forensics tools, and anonymous repositories of incidents open new horizons for the incorporation of CH practices in utilities where they have not been used before. Our analysis shows that existent cybersecurity and cyber hygiene maturity models cover common CH practices and allow us to measure the general maturity level but do not take into account the level of adoption of core cybersecurity components used by Smart Grids organizations for (i) detection (e.g., SPEAR SIEM); (ii) forensics (e.g., SPEAR FRF); (iii) information sharing (e.g., SPEAR RI) in the Smart Grid protection cycle.

To be in compliance with the CH rules related to the Smart Grids, we deliver a cyber hygiene maturity assessment framework tailored to the Smart Grid protection cycle by extending general CH frameworks with Smart Grid infrastructure indicators, which is both maintainable and upgradable in terms of adoption for the Smart Grids cybersecurity components. Special components in the section of people indicators (awareness, education, and training) are also introduced. Therefore, the proposed extension goes one step further by focusing on CH in the Smart Grid.

RESULTS

A cyber hygiene maturity model (CHMM) is a benchmark that customers can use to assess a Smart Grid cybersecurity practices landscape, whether in relation to people, process, technology, or all three.

The CHMM enables performing CH maturity assessment and identifying gaps between the current and future state. SPEAR promotes the use of the Smart Grid CHMM to help end-users (Smart Grid operator organizations) understand quantitatively where they are (an as-is state) in terms of cyber hygiene posture and, based on their mission and goals, where they want to be (a to-be state).

The CHMM gets relevance as a tool to aid the organizations in measuring the progress on the adoption of best practices and technologies supporting prevention, detection, and reaction against cyber threats in their systems. The specificities of the SPEAR CHMM reside in the fact that it is tailored to the needs of Smart Grids systems and organizations operating them and in the fact that it fully aligns with SPEAR solution methodologies (e.g., SPEAR Forensics Framework) and tools (e.g., SPEAR SIEM) to support some of the CH best practices and recommendations promoted in the model. A maturity assessment provides an indication of strengths, weaknesses, opportunities, and threats.

The target audience for the CHMM includes Smart Grid infrastructure or service operator organizations, policymakers, system integrators, cybersecurity and information security specialists, architects, security assessors, regulatory authorities, analysts, and other stakeholders involved in the processes of the development and implementation of mature security of the specific Smart Grid system.

Adoption of P-D-C-A Cycle in the SPEAR CHMM

As was shown in previous sections, all maturity models are based on the Plan-Do-Check-Act (P-D-C-A) cycle. The levels of the CHL should include the check items about whether these activities (steps) are following P-D-C-A: defining requirements/plan with objects; carrying the action accordingly; checking whether the implemented actions are working well; acting to correct any deviations toward actually fulfilling the objectives. The basic level includes P & D detection; advanced: P-D-C—Detection & Forensics (P, D) and information sharing; highest: advanced P-D-C-A (continuous improvement) —Detection, Forensics, information sharing.

As was shown in previous sections, all maturity models are based on the Plan-Do-Check-Act (P-D-C-A) cycle. The levels of the CHL should include the check items about whether these activities (steps) are following the P-D-C-A approach. Here, P stands for "requirements or plan defined with objectives," D stands for "do or carry out the actions according to the plan," C stands for "check whether the implemented actions are working well," and A indicates "act to correct any deviations toward actually fulfilling the objectives." The CHMM suggests that while organizations in basic cyber hygiene levels usually only perform P and D activities, they progressively improve in cybersecurity and perform quality checks (C activities) in relation to adopted practices and finally, they are able to follow a continuous improvement approach with A type of activities. In general, organizations in basic CHLs only carry out basic cyber awareness and cyber incident detection practices, while advanced levels correspond to organizations that, besides detection, perform more sophisticated activities such as cyber incident forensics and information sharing. At the highest CHL, we could find organizations that perform all cybersecurity practices in a proactive way, establishing objectives for all of them, continuously assessing their effectiveness, and correcting any digression.

This approach is aligned with the lifecycle of an organization's cybersecurity risk management described in the NIST Cybersecurity Framework (CSF) (NIST Cybersecurity Framework, 2020). Accordingly, it can be easily adopted for Smart Grid CH enabling the progressive adoption of best practices and solutions on different steps in the protection of the Smart Grid system, which are organized by the NIST Cybersecurity framework (2020) in these functions: IDENTIFY-PROTECT-DETECT-RESPOND-RECOVER.

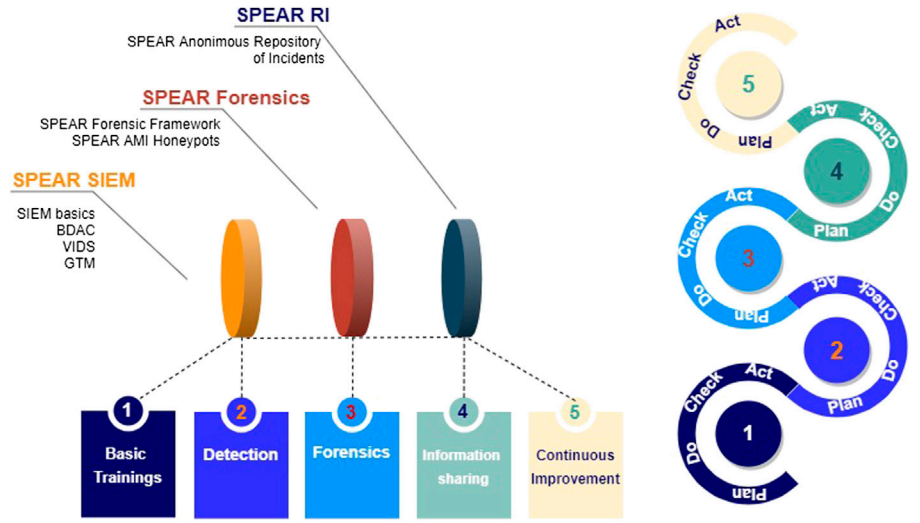

FIGURE 4 | SPEAR CH improvement cycles.

TABLE 1 | Plan-Do-Check-Act coverage of the SPEAR tools on each CHL of the SPEAR CHMM.

P-D-C-A	SPEAR tools	Level 1	Level 2	Level 3	Level 4	Level 5
Plan		+	+	+	+	+
Detection and situational awareness about cyberattacks	SPEAR SIEM		+	+	+	+
Forensics	SPEAR FRF			+	+	+
Information sharing	SPEAR RI				+	+
Continuous improvements	SIEM+FEF+RI					+

Applying a Plan-Do-Check-Act approach in each of the levels of the SPEAR CHMM (see **Table 1**), we can leverage the following procedures supported by SPEAR methods and tools: detection (using SPEAR SIEM), forensics (using SPEAR FRF), and information sharing (SPEAR RI) in the Smart Grid protection cycle (**Figure 4**).

Description of the SPEAR CH Maturity Model

General Structure of the Model

The SPEAR CHMM framework organizes processes and cyber hygiene best practices into three main domains or dimensions of the model: people, organization, and infrastructure. The aggregation of the levels assessed in these domains through the correspondent metrics evaluates the overall maturity level achieved by the organization. The 3×3 domains of the SPEAR CHMM (**Figure 6**) correspond to the following base components of the Smart Grid assessment: (i) Smart Grid infrastructure: in this dimension, the maturity of adopted cybersecurity measures to protect the infrastructure is assessed (e.g., SPEAR tools); (ii) organization: this dimension corresponds to the maturity of the organizational processes (policies, standards, etc.); (iii) people dimension representing the human factor (end-users, operators, and personal of Smart Grids): in this dimension, awareness and training maturity are the main factors of security practices adoption.

SPEAR CHMM consists of five maturity levels (**Figure 6**) ranging from Level 1, Basic, to Level 5, Proactive. Each maturity level is associated with a set of sustainable processes and practices. Practices vary from Level 1, where basic reactive cybersecurity measures (e.g., incident response plan) are developed and step-by-step enhanced, to Level 5, where proactive security is implemented. Respectively, processes could be defined from being introduced at Level 1, properly documented at Level 2, up to being spread across the Smart Grid organization at Level 5. To comply with specific requirements and reach the particular CHL, a Smart Grid organization should implement and completely adopt the processes and practices within the targeted level and below.

The description of the main objectives in each level is summarized as follows.

Infrastructure (Technical Practices)

Level 1: Demonstrate basic CH.
Level 2: Demonstrate intermediate CH + Level 1.
Level 3: Demonstrate good CH and effective security requirements + Level 2.
Level 4: Demonstrate substantial and proactive cybersecurity + Level 3.

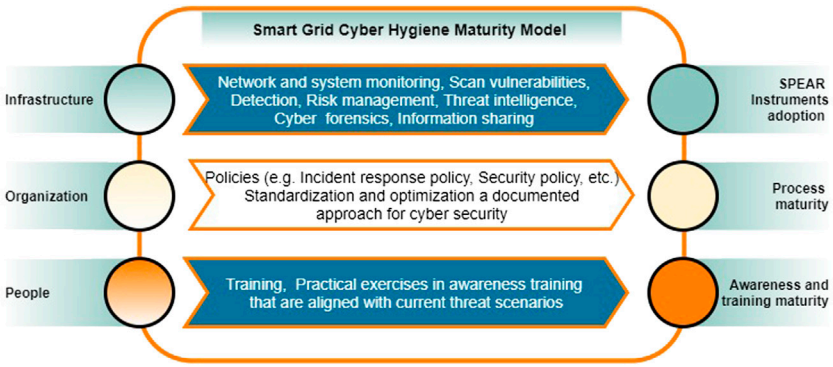

FIGURE 5 | SPEAR cyber hygiene maturity model.

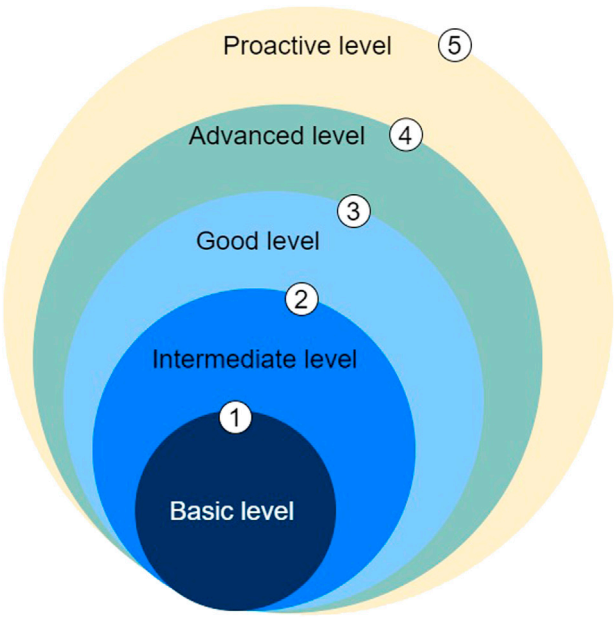

FIGURE 6 | Five levels of cyber hygiene maturity model.

Level 5: Demonstrate the ability of Smart Grid infrastructure to continually evolve to meet cybersecurity threats and repel advanced invasions + Level 4.

Organization (Process Maturity)

Level 1: There is no process maturity.

Level 2: Establish a policy that includes Awareness & Training (AT). Standard operating procedures, policies, and plans are established for all practices.

Level 3: Activities are defined as a standard across the organization. The AT program is actively reviewed for and updated on an annual basis + Level 2.

Level 4: A CH process is tailored for specific departments within the Smart Grid organization. The AT program includes different target groups that have unique training requirements, including skills-based training for IT-department and developer groups. The AT program is actively reviewed and updated on a monthly basis + Level 3.

Level 5: A documented approach for the AT across all Smart Grid units is standardized and optimized across the organization. Activities are identified and improvements are shared + Level 4.

People (Awareness, Education, and Training)

Level 1: Ensure that operators and end-users are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of Smart Grid systems.

Level 2: Document practices to implement the AT. Operators pass security awareness training periodically on recognizing and reporting potential insider threats and using SPEAR SIEM tools + Level 1.

Level 3: Establish, maintain, and resource a plan that includes the AT. A set of training topics focused on general principles of CH in Smart Grid, phishing, social engineering, advanced persistent threat actors, suspicious behaviors, and using SPEAR FRF tool (including demonstrations) is deployed and conducted on a periodic basis. Operators and end-users demonstrate awareness of security risks associated with their activities and of the applicable policies, standards, and procedures related to the Smart Grid security. Smart Grid security team demonstrates awareness of using SPEAR FRF tool + Level 2.

Level 4: Review and measure the AT activities for effectiveness. Training topics include practical exercises in awareness training aligned with current Smart Grid threat scenarios and provide feedback to individuals involved in training and information sharing via SPEAR RI or other SIEM. Department leads and teams request security reviews/audits. Smart Grid security team demonstrates awareness of using SPEAR RI tool + Level 3.

Level 5: The AT is updated at least annually or in case of significant changes to the threat. The leadership actively requests and utilizes security awareness metrics to measure their organizational progress/compare departments across the organization + Level 4.

CH Maturity Levels

Level 1: Basic. This level is considered as basic cyber hygiene and includes a set of cyber protective, defense-related measures. The practices on this level are seen as laying the basis for the higher levels.

Smart Grid Infrastructure indicators: There is no monitoring and sharing data. SPEAR tools have not been adopted.

Organization indicators: There is no security awareness program. No standards are in place and inconsistency exists across the organization.

People indicators: Operators and end-users declare that they aware of security risks associated with their activities and accepted policies and procedures related to the security of Smart Grid systems.

Metrics: none.

Steps to the next level: 1) Identify the set of applicable regulations and standards. 2) Identify the security awareness training requirements. 3) Identify someone to roll out the required security awareness training. 4) Develop or take the AT that satisfies those requirements. 5) Make use of security awareness training. 6) Track and document all participants who complete the training.

Level 2: Intermediate

Level 2 is seen as intermediate CH, offering continuous maturing of Smart Grid organization from Level 1 to Level 3. Compared to Level 1, this includes more advanced policies that enable the increase of the resilience of Smart Grids to cyber threats. Being at this level, a Smart Grid organization defines, documents, and maintains their information security program and clarifies road map and strategic plans to guide the procedures for protecting their assets, systems, and data, at a level greater than the baseline requirements. The AT program is established to meet specific objectives or comply with the audit requirements. In most scenarios, training is conducted on an annual basis. The staff is aware of the CH practices, but in many cases, people are unconfident of the organizational policies and their role in cyber accident prevention.

Smart Grid Infrastructure indicators: SPEAR SIEM tools are adopted and used periodically: I.2.01, the tool(s) that monitor traffic data have been installed; I.2.02, the tool(s) that monitor device logs have been installed; I.2.11, monitoring of traffic data done periodically (at least once a month); I.2.22, monitoring of devices logs done periodically (at least once a month).

Organization indicators: O.2.01, a policy that includes Awareness & Training (AT) is established but not documented; O.2.02, incident response plan exists, but there is no strategic plan and training topics are *ad hoc* and deployed at random times; O.2.03, the AT program has been established. (4) Organization has limited leadership support. Leadership's goal is to invest the minimum resources. (5) Security awareness is only considered during audits. (6) There is little involvement from other departments, such as communications and human resources. (7) Leadership believes that security is purely a technical issue. (8) Training is primarily once a year. (9) Training is limited to computer-based training, with perhaps some occasional support materials during the year.

People indicators: P.2.01, operators and end-users aware of the cybersecurity risks associated with the working activities are familiar with the accepted standards, policies, and procedures; P.2.02, operators pass security awareness training to recognize and report about potential insider threat, as well as on using SPEAR SIEM tools; P.2.12, there is a set of on-time *ad hoc* training topics deployed once a year; P.2.22, operators pass computer-based training periodically, with support materials during the year. End-users feel security is something that IT takes care of and that it is not their problem.

Metrics: (1) Number / % of people that have completed training. (2) Number / % of people that have signed Acceptable Use Policy. (3) Number of on-site training sessions in one year. (4) Number/frequency of awareness materials distributed (newsletters, posters, etc.).

Steps to the next level: 1) Identify stakeholders. 2) Create a CH awareness program and identify scope, goals, objectives, assumptions, and constraints. 3) Identify who will be responsible for the awareness program. A person should be dedicated full-time and have a soft skills background to ensure the greatest success. 4) Create Advisory Board. 5) Identify the target group for the CHL program, starting with a baseline for all employees. 6) Identify what human risks should be managed and the behaviors that will mitigate those risks. 7) Identify how to include cultural analysis, primary training, and reinforcement training. 8) Develop or purchase training materials. 9) Create an execution plan with milestones to include metrics. 10) Have senior leadership announce the plan and execute it.

Level 3: Good Cyber Hygiene

Level 3 involves a certain amount of expertise in protecting and sustaining the main assets of Smart Grid organization. An organization assessed at Level 3 CHMM demonstrates good cyber hygiene and effective implementation of security controls. However, it may face a range of challenges related to eliminating advanced persistent threats (APT). It is expected that for the maturity of the processes, the Smart Grid organization will adequately tap resources and verify compliance with policies and procedures, demonstrating good practices in managing cybersecurity and CH. The AT program is targeted at the most important user groups and learning topics that focus on these key elements of cybersecurity and ensure effective implementation of the organization's mission. The program is regularly updated and includes ongoing reinforcement throughout the year. As a result, people have good understanding of the policies of their organization and are able to recognize, prevent, and report incidents.

Smart Grid Infrastructure indicators: SPEAR SIEM and SPEAR FRF tools are adopted. Metrics describe the level of adoption of SPEAR instruments in Smart Grids: I.3.11, monitoring traffic data is done continuously (at least once a week); I.3.22, monitoring device logs is done continuously (at least once a week); I.3.03, the tool(s) for anomaly detection have

been installed. I.3.13, the tool(s) for anomaly detection are used periodically (at least once a month). Application stability and performance are continuously monitored.

Organization indicators: O.3.01, a policy that includes the AT is fully documented; O.3.02, an incident response plan is fully documented and includes strategic plan and schedule of trainings; O.3.03, a strategic plan that has identified the scope, goals, objectives, and justification for the AT is documented; O.3.05, data back-up policy has been established; O.3.33, organization has clearly defined target groups, usually based on roles/risks but can also be defined by language, region, or other drivers; O.3.43, top human risks, actions, and behaviors that enable sufficiently managing those risks have been identified and explained; O.3.13, the AT program coordinates and collaborates with various departments within the organization, including Communications, Human Resources, and Help Desk; O.3.04, the AT program is actively reviewed and updated on an annual basis; O.3.23, a CH process is defined as a standard across the organization; O.3.14, the AT program includes continuous reinforcement throughout the year.

People indicators: P.3.03, there is an AT program lead who is working on a full-time basis and is responsible for the development, implementation, and updating the AT program. P.3.02, training topics are focused on general principles of CH in Smart Grid, phishing, social engineering, advanced persistent threat actors, suspicious behaviors and using SPEAR FRF tool (including demonstrations) and deployed on a periodic basis. P.3.01, operators and end-users demonstrate awareness of cybersecurity risks related to their activities as well as accepted standards, policies, and procedures. P.3.11, Smart Grid security team demonstrates awareness of using SPEAR FRF tool. P.3.05, training topics include real-life examples and exercises in awareness training aligned with actual threat scenarios, provide information sharing via SPEAR RI, and track the progress of people involved in training. (6) People are reporting incidents or suspected attacks. (7) When the security team pushes out information, people are asking them questions. (8) Employees are exhibiting the behaviors they are being trained on. (9) Employees bring strong security behaviors at home.

Metrics: (1) Phishing assessments. (2) Number of infected computers/devices each month. (3) Number of lost or stolen computers/devices each month. (4) Number of security policy violations.

Steps to the next level: 1) Establish a process to give leadership regular updates on an awareness program. 2) Identify the technological changes, new threats, variations in business requirements, or standards and include all of them in an annual report. 3) Take a poll to determine the current state of awareness and associated behaviors. 4) Schedule a specific date when the security program is reviewed every year and who, what, and how questions are updated by the Advisory Board. 5) Expand modalities to scale and engage the workforce. Examples include gamification and OSINT briefs for senior executives.

Level 4: Advanced

At CH assessment model Level 4, a Smart Grid organization is characterized by substantial and proactive cybersecurity. This means a high level of adaptation of their protection and sustainment activities to the changing methods, techniques, and procedures in use by APT. For process maturity, it is expected that Smart Grid organization reviews and documents all activities related to cybersecurity and timely informs upper executive management about any issues or cyber incidents. The AT program is equipped with all necessary resources and updated at least on an annual basis. As a result, the program becomes a part of internal culture and is relevant, engaging, and up-to-date. The AT program keeps beyond changing behavior and supports people's beliefs, attitudes, and perceptions of security. At a minimum, it takes 3–10 years to achieve this level.

Smart Grid Infrastructure indicators: SPEAR SIEM, SPEAR FRF, and SPEAR RI tools are adopted. I.4.1, monitoring of traffic data is done continuously. I.4.2, monitoring of devices logs is done continuously. I.4.3, forensics is done on anomalies detected. I.4.23, the tool(s) for anomaly detection are used continuously (at least once a week). I.4.04, the tool(s) for information sharing (e.g., SPEAR RI) have been installed. I.4.14, the tools for information sharing are used for sharing information between Smart Grid organizations periodically (at least once a month).

Organization indicators: O.4.23, a CH process is tailored for specific departments. O.4.04, the AT program is actively reviewed and updated on a monthly basis. O.4.13, the AT program includes identified multiple different target groups that have unique training requirements, including skills-based training for IT-department groups and developer groups. O.4.14, reviewing and measuring AT activities for effectiveness are performed on a monthly basis.

People indicators: P.4.02, Smart Grid security team demonstrates awareness of using SPEAR RI tool. P.4.03, department leads and teams request security reviews/audits. (3) Program lead is actively updating leadership on a monthly basis. (4) Security team believes in investing in human controls just as much as technical controls. There is strong integration between awareness and technical practice. Good security practices are "baked in" who we are and what we do. (5) Employees educate others on good security behaviors. (6) Employees start providing ideas or suggestions on how to improve security in the organization. (7) Employees or departments request security briefings/updates; they are actively seeking more information. (8) Department leads and teams request security reviews/audits. (9) Departments beg to compete/compare who has the best security.

Metrics: (1) Number of events analyzed by SPEAR SIEM. (2) Survey measuring people's attitudes, perceptions, and beliefs toward information security and number of people/departments requesting security briefings or updates. (3) Number of people submitting ideas on how to improve security. (4) Number of people attending optional events. (5) Number of requests on how a family can take the training.

Steps to the next level: 1) Create a metrics dashboard that combines all the information/measurements from the different maturity levels. 2) Tie in metrics to technical security metrics and ultimately Smart Grid overall mission.

Level 5: Proactive

At CH assessment model Level 5, a Smart Grid organization has advanced cybersecurity. The organization is capable of adapting its protection activities, changing tactics, updating techniques, and enhancing procedures to have strength against APT. In terms of process maturity, it is expected that the Smart Grid organization reviews and documents all activities related to high-level security management and implementation. The AT program has a robust metrics framework aligned with the organization's mission to track progress and measure impact. The AT program is continuously improving and able to demonstrate return on investment.

This level assumes that SPEAR SIEM, SPEAR FRF, and SPEAR RI tools are completely adopted and periodically updated.

Smart Grid Infrastructure indicators: I.5.24, the tool(s) for information sharing are used continuously (at least once a week). I.5.4, there is information sharing between SG organizations.

Organization indicators: O.5.13, a documented approach for AT across all SG units has been standardized and optimized across the organization (on an annual basis). (2) The process is continuously improved.

People indicators: P.5.02, the training is updated regularly (annually or in case of significant changes to the threat). P.5.03, leadership actively requests and uses security awareness metrics to measure their organizational progress/compare departments across the organization.

Metrics: All the above is combined into a single dashboard interface or some type of centralizing capability that can be visualized and easily reported to business partners. Strategic metrics include the following: (i) number of incidents, (ii) time to detect an incident, and (iii) time to recover from an incident.

Security capabilities metrics can be used to effectively and consistently measure the current CH maturity via information gathering and reporting and compatible testing and evaluate procedures that enable Smart Grids organizations to clearly identify improvement points in order to reach higher maturity levels.

CH Maturity Level Assessment

The CHL maturity assessment procedure usually starts by creating an assessment plan. Then, the assessors collect all the necessary evidence, calculate the maturity levels, and generate the report that details the findings and CH maturity levels for each of the three domains in the CHMM model. Based on the assessment results, the Smart Grid organization can plan the necessary improvements to reach a new maturity level target.

DISCUSSION

The SPEAR Cyber Hygiene Maturity Assessment Framework (CHMF) addresses two major goals in the cyber hygiene playground. Firstly, it enables awareness and adoption of fundamental cyber hygiene practices for Smart Grids and secondly, it guides the Smart Grid operator organizations in the path to progressively adopt measures to boost their overall cybersecurity posture and achieve high CHL with respect to cybersecurity, privacy, and data protection issues. The structure of the model adopted for the SPEAR CHMM is inspired from DoD Cybersecurity Maturity Model Certification (CMMC) v1.02 (of March 18, 2020). The SPEAR CHMM is tailored to evaluate the level of cyber hygiene in Smart Grid organizations since it captures Smart Grid infrastructure and operator organization dimension related cybersecurity practices and aligns with the Smart Grid cybersecurity tools proposed by the SPEAR project. Furthermore, the SPEAR CHMM aims at assuring cyber awareness and readiness of Smart Grid personnel and customers to different cyber threats and cyberattack incidents. To enable the quantitative assessment of the practices associated with each of the CHL, we developed a questionnaire where most of the questions need to be answered with a Yes/No type of responses. The SPEAR CHMM auditor (who could be internal or external staff of the Smart Grid operator organization) would assess the maturity level by making questions oriented to cybersecurity responsible personnel to measure Yes/No availability of practices proposed by the CHMM and in case the practice is measurable, evaluate the metrics of indicator. The final result of the assessment would therefore be the identification of the CHL of the organization, with the results of the values of the metrics measured for each of the practices, and then a report on the recommended activities to carry out or adopt in the organization to progress to the next maturity level so that the organization can increase cyber protection and preparedness against cyber incidents or attacks ENISA Europa EU, 2009.

The SPEAR CHMF enables verifying whether a Smart Grid organization matches the requirements to reach a certain cyber hygiene maturity level and due to a simplified information collection, it can be used to automate CH maturity assessment. The assessment also emphasizes the level of adoption of standards and best practices in CH for each control area and its effectiveness and maturity of internal policies and procedures. As in many risk assessment approaches [The Department of Defense (DoD), 2020; Cybersecurity Maturity Model Certification (CMMC), 2020; U.S. Department of Defense, 2020], assessors in SPEAR CHMF typically evaluate indicators based on whether they are in place or implemented, resulting in a binary Yes/No and compliance-oriented manner.

All of these results have been validated by SPEAR end-users and are currently being reviewed by Smart Grid stakeholders outside the SPEAR Consortium. The methodology and outcome of these evaluations are planned for publication in the near future.

CONCLUSION

This work explains the support offered in SPEAR to improve the CH practices in organizations operating Smart Grids in Europe. We reviewed the CH needs and challenges in the Smart Grid domain and analyzed the state of the art in best practices and standards around cybersecurity and CH in the energy domain. The proposed CHMF integrates the best practices in Smart Grid cybersecurity and cyber hygiene and proposes to organizations a well-organized and structured adoption of cyber practices to increase cybersecurity capabilities. The CHF includes trainings, the CHMM, and a comprehensive approach to measure the progress of capability improvement in Smart Grid organizations according to the levels defined in the CHMM.

The SPEAR CHMM organizes the progress in cyber hygiene capabilities improvement in five levels as described above. The approach proposed is a P-D-C-A cycle where the organizations improve their cybersecurity capabilities in three different dimensions: organization, infrastructure (corresponding to the Smart Grid), and people (organization staff). The CHMM explains the improvement and support that SPEAR tools offer to the different activities proposed in the capability enhancement process.

All the materials provided, including the CHMM and its assessment methodology, have been designed according to the needs, ideas, and suggestions from SPEAR end-users collected through dedicated questionnaires developed in the project as well.

Considering the scope of the CHMM, it is delivered with the following training modules: (i) Cybersecurity awareness for electricity organizations: Smart Grid cyber risks and general cybersecurity rules; (ii) cybersecurity awareness for electricity consumers: recommendations to protect their privacy and basic security rules; (iii) SPEAR SIEM for Smart Grid operators; (iv) SPEAR Forensics [SPEAR Forensics framework; SPEAR AMI Honeypots (RTU honeypots, Smart meter honeypots, etc.)]; SPEAR Information Sharing (SPEAR RI: Anonymous Repository of Incidents).

Supplementary materials present the summary of the assessment items evaluated by the SPEAR CHMF proposed.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/**Supplementary Material**; further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

IB developed the idea and concept, and the CHMF, and wrote the manuscript. IK validated the methodology and checked and analyzed results. EV advised on general leadership, supervised the project, defined the content structure, and provided major corrections to the original draft. All authors exchanged ideas, created, and improved this article. All authors contributed to the article and approved the submitted version.

FUNDING

This project has received funding from the European Union Horizon 2020 research and innovation program under grant agreement No. 787011 (SPEAR)

ACKNOWLEDGMENTS

The authors acknowledge all the SPEAR Consortium for their valuable help in this work.

SUPPLEMENTARY MATERIAL

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fcomp.2021.614337/full#supplementary-material.

REFERENCES

Agence nationale de la sécurité des systèmes d'information (2013). 40 essential measures for a healthy network. Available at: https://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_v1-2-1_en.pdf (Accessed July 8, 2020).

Bertino, E., and Islam, N. (2017). Botnets and internet of things security. *Computer* 50 (2), 76–79. doi:10.1109/MC.2017.62

Blaikie, P., Cannon, T., Davis, I., and Wisner, B. (1994). *At risk: natural hazards, people's vulnerability and disasters*. London, United Kingdom: Routledge.

CIS (2019). Controls Microsoft windows 10 cyber hygiene guide. Available at: https://www.cisecurity.org/press-release/cis-controls-microsoft-windows-10-cyber-hygiene-guide/ (Accessed July 10, 2020).

CORDIS (2020). Community research and development information service (CORDIS) of the European commission. Available at: https://cordis.europa.eu/ (Accessed July 10, 2020).

Cybersecurity Capability Maturity Model (2019). Cybersecurity capability maturity model version 2.0, June 2019. Available at: https://www.energy.gov/sites/prod/files/2019/08/f65/C2M2%20v2.0%2006202019%20DOE%20for%20Comment.pdf (Accessed July 12, 2020).

Cybersecurity Maturity Model Certification (2020). Cybersecurity maturity model certification(CMMC) v1.02 & NIST 800-171 rev2 compliance, 18 March 2020. Available at: https://www.complianceforge.com/cybersecurity-maturity-model-certification-cmmc/ (Accessed July 10, 2020).

Downing, T. E., Aerts, J., Soussan, J., Barthelemy, O., Bharwani, S., Ionescu, C., et al. (2005). *Integrating social vulnerability into water management SEI working paper and newater working paper No. 4*. Oxford, United Kingdom: Stockholm Environment Institute.

Eakin, H., and Luers, A. L. (2006). Assessing the vulnerability of social-environmental systems. *Annu. Rev. Environ. Resour.* 31, 365–394. doi:10.1146/annurev.energy.30.050504.144352

ECS (2018). WG5: education, awareness, training, cyber ranges. Available at: https://ecs-org.eu/working-groups/wg5-education-awareness-training-cyber-ranges (Accessed Jul 8, 2020).

Energy statistics (2017). Energy statistics in Iceland 2017. Available at: https://orkustofnun.is/gogn/os-onnur-rit/Orkutolur-2017-enska-A4.pdf (Accessed July 8, 2020).

ENISA Europa EU (2017a). National cybersecurity strategies—interactive map. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map (Accessed July 8, 2020).

ENISA Europa EU (2009). Good practices on reporting security incidents. Available at: https://www.enisa.europa.eu/publications/good-practice-guide-on-incident-reporting-1/at_download/fullReport (Accessed July 8, 2020).

ENISA Europa EU (2017b). Cyber hygiene. Available at: https://www.enisa.europa.eu/publications/cyber-hygiene (Accessed July 10, 2020).

Greenland Energy profile(2018). Greenland Energy profile 2018. Available at: https://www.indexmundi.com/greenland/energy_profile.html. (Accessed July 8, 2020)

Industrial Internet Consortium (2018). IoT security maturity model: description and intended use IIC:PUB:IN15:V1.0:PB:PB20180409. Available at: https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf (Accessed July 5, 2020).

Inria White Book No. 3 (2019). Cybersecurity. current challenges and Inria's research directions. Available at: https://www.inria.fr/sites/default/files/2019-10/LB_cybersecurity_WEB.pdf (Accessed July 10, 2020).

Linkov, I., Baiardi, F., Florin, M., Greer, S., Lambert, J. H., Pollock, M., et al. (2019). Applying resilience to hybrid threats. *IEEE Secur. Privacy* 17 (5), 78–83. doi:10.1109/MSEC.2019.2922866 Sept.-Oct. 2019.

Miller, F., Osbahr, H., Boyd, E., Thomalla, F., Bharwani, S., Ziervogel, G., et al. (2010). Resilience and vulnerability: complementary or conflicting concepts?. *Ecol. Soc.* 15 (3), 11, 2010 . Available at: http://www.jstor.org/stable/26268184 (Accessed October 5, 2020).

NIST (2020). Cybersecurity framework. Available at: https://www.nist.gov/cyberframework (Accessed Jul 30, 2020).

NIST CAVP (2018). CAVP-Cryptographic Algorithm validation program. Available at: http://csrc.nist.gov/groups/STM/cavp (Accessed Jul 10, 2020).

NIST CMVP. CMVP-Cryptographic module validation program. Available at: http://csrc.nist.gov/groups/STM/cmvp (Accessed Jul 10, 2020).

Norton (2020). Good cyber hygiene habits to help stay safe online. Available at: https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html (Accessed July 8, 2020).

Saed, M., Daimi, K., and Al-Holou, N. (2013). *"Smart grid security concepts and issues, 2013,"* in Proceedings of the World Congress on Engineering 2013, London, United Kingdom, July 3–5, 2013 (WCE 2013).

The Cybersecurity Capability Maturity Model for Information Technology Services (2015). The cybersecurity capability maturity model for information technology services (C2M2 for IT services) v1.0 April 2015. Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/1026943.pdf (Accessed July 12, 2020).

The Department of Defense (DoD) (2020). Cybersecurity maturity model certification (CMMC), "How the HITRUST approach can help organizations demonstrate compliance with and obtain certification under the DoD CMMC program." June 2020. Available at: https://hitrustalliance.net/content/uploads/The-DOD-CMMC.pdf (Accessed July 30, 2020).

The SPARKS Project (2015). Social engineering attacks and the smart grid. Available at: https://project-sparks.eu/social-engineering-attacks-and-the-smart-grid/ (Accessed July 12, 2020).

U.S. Department of Defense (2020). Cybersecurity maturity model certification (CMMC) v1.0, 31 January 2020. Available at: https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf (Accessed July 12, 2020).

U.S. Department of Energy (2014a). Electricity subsector cybersecurity capability maturity model V1.1. DOE, February 2014. Available at: http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-v-11-february-2014 (Accessed July 8, 2020).

U.S. Department of Energy (2014b). Cybersecurity capability maturity model. DOE, February 2014. Available at: http://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014 (Accessed July 8, 2020).

Wang, W., and Lu, Z. (2013). Cyber security in the smart grid: survey and challenges. *Comput. Networks* 57 (5), 1344–1371. doi:10.1016/j.comnet.2012.12.017 URL.

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.