2020 12th International Conference on Cyber Conflict
20/20 Vision: The Next Decade
T. Jančárková, L. Lindström,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2020 © NATO CCDCOE Publications, Tallinn

Addressing the Cybersecurity Challenges of Electrical Power Systems of the Future

Gilberto Pires de Azevedo
Researcher
Electrical Power Systems Dept.
Electric Energy Research Centre
Rio de Janeiro – RJ, Brazil
gilberto@cepel.br

Maxli Barroso Campos
Chief of Division
Strategic Management Dept.
Cyber Defence Command
Brasília – DF, Brazil
campos@cdciber.eb.mil.br

Paulo César Pellanda
Professor
Electrical Engineering Dept.
Military Institute of Engineering
Rio de Janeiro – RJ, Brazil
pcpellanda@ieee.org

Abstract: Electrical Power Systems (EPSs) are among the most prominent critical infrastructures of our digital society. Assets, systems and networks of most other critical infrastructure sectors depend heavily on EPSs and would fail in the event of persistent electricity supply problems. This should make EPSs attractive targets for cyberattacks, so it is somewhat surprising that few large-scale successful cyberattacks on the electricity sector have been reported so far.

EPSs structures are undergoing deep changes that will accelerate over the next years. A convergence of environmental concerns and technological evolution is leading to the widespread use of distributed renewable microgeneration, electric vehicles, distributed energy storage, Internet of Things, smart grids and software-defined operating devices. These game-changing innovations are reshaping EPSs. The previously well-ordered computational environment where a limited number of agents interacted in

predictable ways will gradually receive new layers of agents, where thousands or even millions of them will buy or sell services in a kind of giant open market. The search for individual advantages or profits rather than overall system welfare will guide the actions of these new participants.

This work examines the traditional structure of EPSs from a cybersecurity point of view as well as foreseeable changes. It will also look at associated risks and discuss possible approaches to mitigate them.

Keywords: *critical infrastructure, electrical power systems, soft cybersecurity, industrial control systems, SCADA*

1. INTRODUCTION

Discussions about cybersecurity concerns in electrical power systems (EPSs) quite often have an alarmist approach. Catastrophic scenarios in which cyberattacks produce massive blackouts leading to generalised chaos and substantial economic losses are imagined and described by specialists trying to draw attention to cybersecurity issues in EPSs. However, there are as yet no examples of cyberattacks that have had such drastic consequences, which can lead some sceptical decision-makers to neglect prevention.

It can be said that both views are right to a point. While the possibility of cyberattacks with catastrophic consequences remains small today, it will increase quickly over the 2020s, mainly on the back of the profound transformations taking place in the electricity supply sector. Satisfactory cybersecurity levels are not only a condition for the safe operation of systems but also a crucial requirement for system evolution. Preventive measures to mitigate the vulnerabilities and risks of the new environment are possible and essential, but significant work on research, development, governance and other areas is required to provide and maintain acceptable levels of cybersecurity.

This work starts with an overview of the evolution of EPSs from the perspective of cybersecurity (Sections 2 and 3), followed by a discussion of some foreseeable challenges (Section 4). Possible approaches to tackle those challenges and suggestions for future work are presented in Section 5.

For the sake of conciseness, the abbreviation EPS stands for “electrical power system”, comprising generation, transmission and distribution equipment and, in

some cases, also the associated computational and communication infrastructure. For the same purpose, the text avoids addressing general cybersecurity concepts except when necessary to examine specific details about EPSs. The term "attack" (and hence "attacker" and "cyberattack") is used throughout the text in a broader and more informal sense than defined in [1]. Finally, since multi-agent systems are an appropriate metaphor to represent EPSs of the future, the term "agent" is applied to refer to any active participant of the system that has some degree of autonomy for monitoring the environment, communicating with some other agents and acting to reach its own goals [2, 3].

2. ELECTRICAL POWER SYSTEMS: CRITICAL INFRASTRUCTURE FOR OUR SOCIETY

EPSs are among the most prominent critical infrastructures of our digital society. The assets, systems and networks of most other critical infrastructure sectors depend heavily on EPSs and would fail in the event of persistent electricity supply problems, generating a ripple effect and seriously compromising other critical infrastructures [4].

This should make EPSs very attractive targets for cyberattacks; thus it is somewhat surprising that few successful large-scale attacks have been reported in the electricity sector so far. Nevertheless, a closer look shows that the vulnerability of existing electric power grids to cyberattacks is not too alarming at present, in part due to the relative abundance of old elements with low degrees of computational connectivity, as well as the still small number of different classes of agents that interact via computer networks.

A complementary explanation for the relative success of cyber protection of EPSs today is the still limited motivations for cyberattacks – especially the scant possibility of obtaining economic advantages from them. Unlike from attacks on services such as banking, there are as yet few possible rewards to be gained from attacking EPSs.

As an illustration, one can examine the famous December 23, 2015 cyberattack at Ukrainian Kyivoblenergo [5], a regional electricity distribution company. This incident is often reported as an example of the potential effects of attacks on EPSs. Very sophisticated techniques were applied, and months of preparation were required. Up to 225,000 customers were affected by power outages that lasted several hours; however, the impacts of the incidents were rated as low, as the outages affected a small number of overall power consumers in Ukraine and were limited in duration. Analysis results based on a single incident should not be generalised, but the balance

between the likely effort expended in preparing that attack and its results does not seem to encourage further similar attacks.

Unfortunately, this relatively peaceful scenario will not last for long. EPSs are undergoing profound structural changes that will make cybersecurity a primary concern for system regulators, planners and operators [6] – and not only for them.

3. ELECTRICAL POWER SYSTEMS: DEEP TRANSFORMATIONS TAKING PLACE

EPSs are perhaps the most extensive and complex artificial infrastructures on Earth, but have been evolving slowly and incrementally for decades. Despite changes in governance in some countries, the physical structure of EPSs has remained essentially the same for a long time. Utilities, consumers, regulators and operators have well-defined roles and interact in a well-ordered fashion. Computational systems and communication networks associated with EPS monitoring and control are often isolated from other networks and based on non-standard implementations. Cybersecurity preventive measures are incipient, but prospective cyber attackers have had a small surface of attack available and the possible consequences of successful attacks have tended to be limited in extension and duration.

However, EPS structures are currently undergoing profound changes that will accelerate in the coming years. A convergence of environmental concerns, technological evolution and other drivers will reshape EPSs over the next decades:

a. The uncertainty in the availability of generation due to the widespread use of intermittent distributed renewable generation like wind and photovoltaic;
b. Expected advances in distributed electricity storage technology;
c. Electric vehicles that might behave either as moving loads or electricity storage devices;
d. New roles for consumers, who will gradually change their passive behaviour to act also as small energy producers and energy stores; they will also be able to autonomously control their demand in response to dynamic energy prices or similar indications;
e. Internet of Things, 5G and other innovations will connect vast numbers of sensors and control devices to EPSs. Even some domestic apparatus will be connected and respond with a certain degree of autonomy to external signs and demands.

The drivers behind these transformations in EPSs are often grouped under the so-called "3-Ds" view: digitalisation, decarbonisation and decentralisation. Smart grid, autonomic power systems [3] and multi-agent systems [7] are concepts that provide abstractions that help to handle the complexity of the future EPS environment [9].

A. New Layers of Agents

Long-established EPS actors like utilities, customers, operators, regulators and similar ones [9] could be classified as the "first layer" of agents; the "second layer" would encompass new classes of agents that are just starting to take part in the electrical power system such as distributed microgenerators, electric vehicles and storage units [9]; "third layer" agents would include, among others, associations of agents of previous layers; and the "fourth layer" includes providers of services for associations of agents, etc. The resulting environment will be diversified, probably following this proposal for stratification in different layers, with a number of agents far greater than that of the existing "first layer". The previously well-ordered computational environment where a limited number of agents interacted in predictable ways will coexist with – or be replaced by – a much more complex one where a vast number of agents will buy or sell services in a kind of giant open market. In [3], the author mentions "the potential for hundreds of millions of devices across Europe to be involved in the electricity market and to contribute to network operation through demand response" by 2050. The search for individual advantages or profits rather than overall system welfare will guide the actions of most of these new agents.

By the early 1990s, when the internet took its first steps outside research institutions, it was already clear to many that it was a habitat where a plethora of new businesses would emerge and evolve in a very different way than in the physical world. However, despite a handful of evident candidates (news, banking, marketing, commerce and a few others), at that time no one could have predicted the extraordinary diversity of new businesses that would appear on the internet, nor the associated risks. Electrical power system researchers and planners are currently in a situation that resembles that of internet pioneers: while it is evident that many new businesses and agents will start to have active roles in the system in the coming years, it is challenging to guess precisely who they will be and how tightly controlled the environment where they will interact will be.

In short, the expected transformations suggest that EPS cybersecurity professionals will have to deal with an increase in both cyber vulnerabilities and attack surfaces, with widespread connections to potentially insecure external networks, and with explosive numbers of new and relatively independent active agents.

B. Increasing Criticality of SCADA Systems

SCADA ("supervisory control and data acquisition") systems are often part of industrial control systems (ICS) that monitor and control industrial processes. Few of these processes are as relevant to our society as EPS control, where SCADA systems are the main actors. Due to their criticality, they deserve special attention in any cybersecurity analysis.

Early generations of SCADA systems were built over proprietary technologies and often used customised versions of communication protocols; connections to the internet were rare. Although cyber protection measures were almost non-existent, those SCADA systems were relatively protected from cyberattacks by a combination of "security through obscurity", small surface of attack and limited motivations for cyber attackers.

As mentioned earlier, this peaceful landscape is changing rapidly. SCADA systems are now directly or indirectly connected to the internet, use standard communication protocols, and proprietary technologies have been replaced by commercial software packages and operational systems. Despite providing significant reductions on development and evolution costs and schedules, improving maintainability and favouring interoperability, in theory these changes could make SCADA systems increasingly vulnerable to even generic malware attacks. Adding to this scenario the increased motivations for attackers, SCADA systems will face significant cybersecurity challenges.

Frameworks like the Purdue Model for Control Hierarchy [8] provide good starting points for the segmentation of EPS control systems, including SCADA, and help to build more secure environments by defining zones with different protection requirements. It is likely that such frameworks will need to be expanded to cover the interactions of SCADA with some of the agents of layers two through four mentioned previously. Interactions with them will significantly differ from others like those with process devices or elements in corporate networks, thus demanding the definition of specific security requirements.

The specificities of the cybersecurity of SCADA environments, discussed below, are sometimes not well understood by professionals of other areas to which those systems are now connected, such as corporate networks. The "availability-first" approach, whereby service continuity is far more important than data confidentiality or even data integrity, may clash with corporate cybersecurity policies.

4. CYBERSECURITY CHALLENGES OF THE EPSs OF THE FUTURE

A. Cyberattacks: Motivations and Targets

It should be noted that there are no significant difficulties in making successful low-tech physical attacks on the electricity grid. Transmission facilities, for example, can be dropped down with simple tools, and simultaneous coordinated attacks on a few strategic transmission lines can lead to severe and long-term outages. The rarity of such attacks suggests that, in peacetime, there are not many motivations for triggering broad and unfocused power shutdowns.

However, in EPSs of the future, increasing cyber vulnerabilities, attack surfaces and severity of effects, and the feasibility of remote attacks without immediate risk to attackers, are likely to reinforce the motivations of cyberattacks. War, terrorism, vandalism and different brands of radical activism are some ordinary motivations for cyberattacks that could be aimed at causing large-scale electricity shutdowns. Other motivations related to criminal activities might also gain relevance. The extortion of power utility companies through threats of cyberattacks that could cause power outages is another example of a set of new options that cybercriminals might try to exploit; new successful criminal "business models" can appear at any time.

Advances in smart grid, Internet of Things and digitalisation in general are opening doors to sharply focused attacks with a renewed set of motivations such as revenge, privacy breaching, harming business competitors and cyber versions of ordinary crimes. For instance, a hacker may try to remotely turn off the heating system of his ex-girlfriend's home, shut down the electricity of an obnoxious neighbour, produce overvoltage to damage equipment of a competitor, or steal credits from microgenerators. Such focused cyberattacks can become very common if insufficient preventive measures are taken.

On the other hand, as mentioned before, advances in the use of commercial software on SCADA systems and other EPS control systems can make them vulnerable to generic malware attacks with motivations that are not related to EPSs.

B. Beyond Cyberattacks

The new EPS scenario described in the previous section, besides bringing new motivations and opportunities for cyber attackers, adds myriad agents that could hardly be called "attackers" but may behave in ways that would harm other agents or even the whole system [9]. A few examples are:

a. Formerly well-behaved agents that are facing temporary problems and thus unable to respond appropriately to requests from other agents, or have had their behaviour degraded permanently whether intentionally or not;
b. Rogue agents offering services that they are unable to provide adequately, due to quantity, quality, or timing issues;
c. Agents trying to mislead their customers to increase their revenues;
d. Agents acting to harm competitors using unfair methods;
e. Agents trying to obtain advantages or revenues illegally.

There will likely be other examples of ill-behaved agents in the EPS of the future. This situation may be a novelty for EPS professionals accustomed to well-controlled computational environments, but not for internet professionals familiar with the risks of open environments. Soft cybersecurity metrics like trust and reputation can help in such environments, as will be seen later.

C. Cyber Operations Against EPSs

Despite fortunately being one of the least common kinds of attacks, cyber operations [1] against EPSs are serious concerns and require a wide range of defensive measures (offensive actions are not discussed in this work). Such operations are likely to be conducted by terrorists, military personnel or sectors of a foreign government. An operational target might be a set of critical cyber infrastructures that include EPSs, an EPS itself, or a more specific objective, such as part of an EPS that feeds power to a specific city, industry or military facility. Sections of an EPS that supply power to military command and control facilities or to weapon systems are also among some preferential targets. Unlike during the Cold War when there were "demonstrations" of the effect of new military technologies, so far cyber operations have tended to be apocryphal [10].

The growing interdependence between critical infrastructures – such as EPSs and communication networks – increases vulnerabilities and the complexity of cyber defence planning. Since technical, practical and economic reasons make it impossible to guarantee comprehensive protections for all critical infrastructures against all threats and risks, identifying key vulnerabilities and infrastructures and critical points to be protected is essential [11].

The evolution of EPSs requires a specialised treatment to identify new intra- and interdependencies. Protecting key elements like SCADA systems, operators and communication networks will no longer suffice as a growing number of new small agents will begin to play active roles in EPSs. These new agents, who will most likely operate based on lower cybersecurity levels, will be easier targets for cyberattacks. Large-scale attacks conducted against thousands or millions of them could lead an

EPS into chaos due to the increasing dependence of EPSs on those small agents. In the long term, those agents should be included in EPS risk analysis and defence strategies.

5. ADDRESSING CYBERSECURITY CHALLENGES

Enhancing EPS cybersecurity requires a broad and diversified range of actions. Grouping them into a few categories, as shown below, can help the analysis.

A. Hard Cybersecurity

Hard cybersecurity refers to mechanisms like access control, authentication, malware control, encryption and other functions commonly used in most computational networks. These are essential cybersecurity tools but are not enough for EPSs: if they fail – and sometimes they do fail – some critical elements of the system may become unprotected. Most hard cybersecurity threats (outdated or poorly configured software, weak passwords, excessive privileges, physical access to critical cybersecurity devices, non-cybersecurity-aware teams, social engineering and many others) are not specific to EPSs and can be fought by well-known strategies. In this work, the hard cybersecurity specificities of EPSs are examined.

One of them is the relative order of importance of the three highest-level goals of cybersecurity [12], namely confidentiality (information is accessed only by authorised agents), integrity (information is changed only by authorised agents) and availability (non-authorised agents cannot substantially harm the behaviour of the network) – the CIA triad. In some business sectors, integrity or confidentiality are often the most important goals. A bank can, in extreme contingencies, temporarily interrupt its online services to avoid interference or damage to its databases; a health insurance company can do the same to preserve the confidentiality of its records. In EPSs, however, availability is paramount and any cyberattack-fighting approach that requires interruption of services is unacceptable.

Cybersecurity policies and strategies must consider the importance of availability and deal properly with associated side-effects. One side-effect is related to the presence of outdated equipment and software co-existing with other equipment in a real-time operational environment. Due to the long lifespan of power system computational hardware and even software, it happens that, during a product lifecycle, suppliers stop providing updates and support or even abandon the market, thus leaving products running outdated versions that are potentially vulnerable to cybersecurity threats. Trying to update these products often brings risks of serious operational problems and raises availability concerns, therefore a common approach is to keep them operating as long as they are performing satisfactorily and to be aware of the risks. To avoid

this uncomfortable and dangerous situation, designers should consider the ease of component replacements from the design phase. Plans to deploy a new component in a system – hardware, software, communication protocols or others – should include a well-documented, simple and smart strategy for its replacement in future.

Another characteristic of EPSs is that they often rely on extensive and poorly monitored communication networks. It is hard to fully prevent physical access to those systems and a single direct connection to a vulnerable point could bypass layers of cyber protection and provide privileged access for attackers. Preventing and monitoring physical access to control and communication hardware is especially important in the presence of outdated hardware or software with insufficient protection against unauthorised accesses, but not only in this case. The possibility of unauthorised direct connections to EPS communications networks should not be neglected and requires appropriate protective measures.

Access to communication networks paves the way for a type of sophisticated attack that has been the subject of much research in recent years: the injection of false data into the measurement network, thus compromising the integrity of the information on which the system's operation is based. This type of attack requires subtle adulterations in some of the field measurements that are received and processed by the state estimator (a software that performs in real time the best possible estimate of the system's state from the measurements received) in order to deceive the supervisory system and take the power system to the state desired by the attacker: unsafe, failure, one that generates undue economic advantages or losses, etc. Detection and prevention of this kind of attack has been the subject of several publications (see [17], for instance).

Other strategies that are not specific to EPSs are especially relevant in this context. Early detection of potentially hazardous behaviour is of great interest and deserves special attention. Honeypots or honeynets developed for real-time control environments can prevent attacks and produce statistics that help refine cybersecurity, and anomaly detection techniques can help to identify suspect behaviours. On the reverse side of the same problem, forensic analysis of attacks (successful or not) is important to retrieve information to improve prevention and to substantiate punitive procedures. Storing enough information for forensic analysis in EPSs, where high rates of information traffic are usual and attacks can take months to prepare, is an issue that merits special attention.

B. Soft Cybersecurity

As seen previously, new "layers" of agents will start to play active roles in EPSs [9]. Many agents, primarily motivated by the expectation of personal profits or advantages and with a significant degree of freedom, will start operating autonomously in power

systems. It can be assumed that some of them will behave in ways that could harm other agents or the whole system, and it is useful to identify them.

In human societies, social mechanisms like reputation and trust reduce the influence of participants that do not behave in a suitable manner; their equivalents in multi-agent systems are the soft cybersecurity mechanisms. The introduction of these mechanisms can be done over solid foundations [13, 14] as they have been used in areas like e-commerce for years.

Reputation evaluation systems, despite some imperfections, have proven effective in motivating agents to behave well and in identifying those that do not. They usually allow parties that have been involved in a transaction to rate each other after its completion. These ratings are then used to construct indexes that are intended to help other agents to decide whether or not to interact with them in future [14].

Differently from reputation, which is built collectively, trust is essentially a personal notion. One agent can even choose to trust another one with a poor reputation, and vice versa. It is also a multifaceted concept that can be split into several classes [13]. The definition of trust that is more appropriate to EPSs is "decision trust" [14, 15]:

> *"Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible."*

This definition indicates that taking risks is an integral part of the concept of trust. It also shows that trust is context-dependent: an agent can choose to trust in another in a specific situation, but not in a different one. The definition also indicates that trust evaluation depends on a balance of potential gains and losses involved in a transaction: when the potential losses are small and the potential gains are significant, one can choose to trust a partner that one would usually not trust. Even if the concept of trust seems to be inherently fuzzy, it needs to be converted to binary values: an agent must decide whether a potential partner is or is not trustworthy enough to engage in a particular transaction.

Application of trust and reputation concepts to the upper layers of future EPSs [9], where thousands or millions of different agents with different capabilities and goals will interact, is not straightforward and is more complex than in the realm of e-commerce. Due to the large number of variables still undefined today, it is debatable whether an early effort to develop attempts at realistic simulations for study purposes would be productive. However, it is likely that the overall system behaviour would benefit from research in this area.

C. High-level Coordinated Actions

High-level coordinated actions are essential components of the defence strategy against some types of cyberattacks, whether directed at EPSs or embracing other critical infrastructure. Inter-agency joint and combined exercises should be centrally coordinated and involve different public and private partners, including those sectors of the armed forces and government responsible for the cyber defence. The engagement of different sectors of society assists in building a robust cybersecurity community capable of exchanging experiences and good practices, and of establishing protocols for information sharing and cooperative work. This may prove essential in crisis situations; otherwise, even the exchange of basic information can be difficult.

There are several initiatives of joint exercises around the world, such as Cyber Europe, a pan-European cyber crisis exercise organised by the European Union Agency for Cybersecurity (ENISA); Cyber Perseu in Portugal, coordinated by the Portuguese Army; the UP Kritis in Germany, conducted by governmental authorities and industry; and the Cyber Guardian in Brazil since 2017, under the coordination of the Cyber Defence Command (ComDCiber). These exercises help to promote collaboration and information exchange at national or supranational levels.

The evolution of EPSs over the next decades and their emerging cybersecurity challenges discussed in previous sections will need to be gradually included in those exercises. They will have an impact on the simulation of scenarios and cyberattacks and bring new vulnerabilities to be reproduced; crisis management, incident response and actions plans must evolve accordingly.

D. Effective Governance in Cybersecurity

Effective cybersecurity governance in EPSs should ideally encompass government, defence, agencies related to EPSs and other critical infrastructure sectors, customers, utilities, private sector representatives, academia and civil society. The digital resilience of EPSs – which is the primary goal of EPS cybersecurity – should be gradually taken to nearly the same level of relevance as EPS energetic supply security or electric operational stability, making cybersecurity a C-suite issue. Cybersecurity managers must also have expertise in topics such as risk and compliance management, corporate governance and overall business objectives. Direct access to senior corporate management is also a must, and all relevant EPS-related agents should adapt to these requirements.

Some important lessons learned indicate risks that should be avoided: (i) excessive securitisation and militarisation of cybersecurity; (ii) exclusion of non-state actors from cybersecurity governance, priority setting and policy-making; (iii) solutions

that seek to block applications, remove content and criminalise behaviours; and (iv) coordination problems within institutions.

The institutionalisation of EPS cybersecurity would ideally encompass technical entities that contribute to the development of related policies, standards and practices. Frameworks for the certification of products, processes and services of interest to EPSs, including concerns with cyber risks brought about by 5G, are also necessary.

Such measures can help to improve the cybersecurity of current EPSs; however, they are insufficient to meet all future needs. The cybersecurity governance of the new layers of autonomous agents is an open issue that deserves special attention as those newcomers will become the weakest link in the cybersecurity chain.

E. Cybersecurity Due Diligence

It may already be a challenge for EPS companies to identify and protect all their critical assets, which can depend on vast, far flung and complex global supply chains. However, the problem is compounded by the ever-increasing degree of digital interconnection with other companies because concerns about cybersecurity can be as different as the companies themselves. For example, a company that builds and operates a set of separate transmission lines (an approach that is part of the EPS business model in some countries) could be much less concerned about cybersecurity than the utilities to which the lines are connected or the national EPS operator. Since the operational networks of those companies are connected to exchange real-time information and commands, a weak link could compromise the cybersecurity of the whole system.

Due diligence of the connection points with other companies is recommended, as well as the definition and enforcement of proper standards to be followed by all parties. And, considering that in some countries the purchase, sale, split and merge of EPS companies are routine, a well-planned cybersecurity due diligence strategy would help provide more agile and orderly evaluation processes.

Extending due diligence strategies to the new layers of EPS agents is a challenge that will probably need to rely on the definition of good and specific connection standards.

F. Staff Awareness and Training (IT and OT)

Sharp differences in cybersecurity approaches do not only occur between different EPS companies; they often exist inside the same utility. Priorities of corporative information technology (IT) staff concerning cybersecurity can greatly differ from those of the teams of real-time operation and SCADA systems (operational technology – OT), and the mutual lack of knowledge about the other environment

brings difficulties and risks. As mentioned before, in real-time control environments the availability of information is much more important than its confidentiality, and even short unplanned interruptions are usually a significant issue that can lead to problems on the energy supply.

The increasing connection between IT and OT environments makes it essential to bridge the gap between their respective cybersecurity teams. In EPS utilities, cybersecurity should be viewed from a broader perspective related to the protection of critical infrastructure, of which the cybersecurity of both operative and corporative networks is part. Drawing up proper awareness and qualification plans for IT/OT professionals should narrow the gap, but it requires a common curriculum that promotes multidisciplinarity. Joint work of IT/OT professionals, as in incident handling teams, is necessary since both environments are increasingly interdependent and connected. Extending this approach to the armed forces or other organs responsible for the cyber defence of critical infrastructure improves their effectiveness because they need well-trained professionals with extensive knowledge of the subjects to be protected who are able to work in cooperation with other experts.

G. Threat Intelligence as a Service

The development of malware, espionage or even cyber weapons is greatly facilitated by the Dark Web [16] and the anonymity that it provides. Effective cyber exploits are monetised and sold in specialised markets, and threat agents that do not have the technical ability required to build specific "tools" can now buy the desired features and hire additional developments.

The development of threat intelligence as a service (ThIaaS), using methodologies such as data mining and machine learning, can help EPS agents to identify, mitigate and prevent attacks, security incidents and other vulnerabilities faster and more efficiently. This service could be leveraged by national or supranational cybersecurity centres and based on an international collaborative environment.

An important support to a network of EPS threat intelligence would be the use of distributed SCADA honeypots and honeynets. Their relevance is expected to increase and, despite the development and monitoring costs involved, they deserve more attention than they have received so far.

H. Research and Development

Research and development (R&D) activities are essential in rapidly evolving technology domains such as cybersecurity. This is even more evident in the case of EPSs, where the physical system itself is changing. Some important research subjects are common to other cybersecurity application domains, like threat intelligence and

topics of artificial intelligence, machine learning, big data analytics and others; other R&D subjects are more specific to current or future needs of EPSs as soft cybersecurity, SCADA honeynets, monitoring of motivations for attackers, visualisation tools for situational awareness etc.

6. CONCLUSION

EPSs are undergoing deep changes driven by forces that can be grouped under the triad of decarbonisation, digitalisation and decentralisation. Some of them are likely to have a strong impact on EPS cybersecurity, such as the multiplication of autonomous agents with active participation in systems and increased vulnerabilities and motivations for attackers.

The new generation of EPS structures is in its infancy, but will hopefully allow the definition and application of satisfactory levels of openness and interoperability with robust cybersecurity in terms of appropriate policies, technologies and processes and well-trained teams. Early actions in this direction could prevent the development of a chaotic and unsafe environment that would resemble the current internet.

In this work, a non-exhaustive list of foreseeable imminent EPS structural changes is presented and discussed from a cybersecurity perspective, including the resulting risks and possible approaches to mitigate them. Accurately predicting all future structural transformations of EPSs and related new cybersecurity challenges and needs is a very difficult task. Nevertheless, developing tools and technologies for effective cybersecurity governance at all layers of new EPS agents and promoting intensive R&D activities to provide technical responses to emerging challenges are some of the right strategic actions to face the huge uncertainties that the industry 4.0 paradigm will bring to EPSs in the near future.

ACKNOWLEDGEMENT

The authors of this paper thank Marcelo Malagutti (PhD Visiting Research Student at King's College London) for his comments, suggestions and revisions.

REFERENCES

[1] M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017.

[2] M. Wooldridge and N. Jennings, "Intelligent Agents: Theory and Practice," *The Knowledge Engineering Review*, vol. 10, no. 2, pp. 115-152, 1995.

[3] S. D. J. McArthur, P. C. Taylor, G. W. Ault, J. E. King, D. Athanasiadis, V. D. Alimisis and M. Czaplewski, "The Autonomic Power System Network Operation and Control Beyond Smart Grids," in 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), pp. 1-7, Berlin, 2012.
[4] K. Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," *Information Security Journal: A Global Perspective*, vol. 18, no. 1, pp. 1-7, 2009.
[5] R. M. Lee, M. J. Assante and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," *Electricity Information Sharing and Analysis Center & SANS Industrial Control Systems Report*, March 18, 2016. Available at http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
[6] European Commission, "Commission Recommendation (EU) 2019/553 of 3 April 2019 on Cybersecurity in the Energy Sector," *Official Journal of the European Union L 96/50*, 5 April, pp. 50-54, 2019.
[7] S. D. J. McArthur et al., "Multi-Agent Systems for Power Engineering Applications - Part I: Concepts, Approaches, and Technical Challenges," *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 1743-1752, 2007.
[8] L. Obregon, "Secure Architecture for Industrial Control Systems," *SANS Institute Information Security Reading Room*, pp. 1-25, 2015. Available at https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327.
[9] G. P. de Azevedo, "Distributed Energy Resources and the Smart Grid: The Role of Cybersecurity," *Accepted for presentation at Cigré 2020 Paris Session*, August 2020.
[10] S. C. da Cruz Junior, "Cyber Security and Defence in Brazil and a Revision of the Strategies of the United States, Russia and India for the Virtual Space (in Portuguese)," Institute of Applied Economic Research (IPEA), Brasília, 2013. Available at http://hdl.handle.net/10419/91261.
[11] M. D. Cavelty, "Critical Information Infrastructure: Vulnerabilities, Threats and Responses," *Disarmament Forum*, UNIDIR, Issue 3, pp. 15-22, 2007.
[12] D. Kapellmann and R. Washburn, "Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure," In Proc. 11th International Conference on Cyber Conflict: Silent Battle, NATO CCD COE Publications, pp. 1-23, Tallinn, 2019.
[13] J. Sabater and C. Sierra, "Review on Computational Trust and Reputation Models," *Artificial Intelligence Review*, Springer, vol. 24, no. 1, pp. 33-60, 2005.
[14] A. Josang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," *Decision Support System*, Springer, vol. 43, no. 2, pp. 618-644, 2007.
[15] D. H. McKnight and N. L. Chervany, "The Meanings of Trust," *Technical Report MISRC Working Paper Series 96-04*, University of Minnesota, Management Information Systems Research Center, 1996.
[16] R. Koch, "Hidden in the Shadow: The Dark Web – A Growing Risk for Military Operations," In Proc. 11th International Conference on Cyber Conflict: Silent Battle, NATO CCD COE Publications, pp. 1-24, Tallinn, 2019.
[17] X. Li and K. W. Hedman, "Enhancing Power System Cyber-Security with Systematic Two-Stage Detection Strategy," *IEEE Transactions on Power Systems*, vol. 35, no. 2, 2020.