Alma Mater Studiorum · Università di Bologna

SCUOLA DI INGEGNERIA E ARCHITETTURA

Corso di Laurea Magistrale in Ingegneria Informatica

STATE OF THE ART AND FUTURE PERSPECTIVES ON SECURITY METRICS AND THEIR APPLICATIONS

Relatore:
Prof.
Marco Prandini

Candidato:
Giacomo Gori

Sessione II
A.A. 2021/22

Abstract

In modern society, security issues of IT Systems are intertwined with interdisciplinary aspects, from social life to sustainability, and threats endanger many aspects of everyone's daily life. To address the problem, it's important that the systems that we use guarantee a certain degree of security, but to achieve this, it is necessary to be able to give a measure to the amount of security.

Measuring security is not an easy task, but many initiatives, including European regulations, want to make this possible. One method of measuring security is based on the use of security metrics: those are a way of assessing, from various aspects, vulnerabilities, methods of defense, risks and impacts of successful attacks then also efficacy of reactions, giving precise results using mathematical and statistical techniques.

I have done literature research to provide an overview on the meaning, the effects, the problems, the applications and the overall current situation over security metrics, with particular emphasis in giving practical examples.

This thesis starts with a summary of the state of the art in the field of security metrics and application examples to outline the gaps in current literature, the difficulties found in the change of application context, to then advance research questions aimed at fostering the discussion towards the definition of a more complete and applicable view of the subject. Finally, it stresses the lack of security metrics that consider interdisciplinary aspects, giving some potential starting point to develop security metrics that cover all aspects involved, taking the field to a new level of formal soundness and practical usability.

Working on this research project, I wrote two paper:

- Metrics for Cyber-Physical Security: a call to action [31], for the International Symposium on Networks, Computer and Communications (ISNCC) 2022, technically co-sponsored by the IEEE
- Towards the Creation of Interdisciplinary Consumer-Oriented Security Metrics[UNDER REVIEW], for the IEEE Consumer Communications & Networking Conference (CCNC) 2023.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In recent years information systems are exposed to an increasing amount of cyber-threats that endanger the daily life of everyone: McAfee estimates that the damages associated with cybercrime now stands at over $400 billion, up from $250 billion two years ago, and the global losses up to 1 trillion[1]. Attackers have a lot to gain from successful data breaches that occurred in the past, hacking tools more and more simple to use and available to everyone, Information Systems that, with the growing of Internet of Things (IoT) devices, are taking part in every kind of human activity (e.g. smart cities, smart home, smart transportation,..) considerably increasing the attack surface and the possible dangerous outcomes of successful attacks.

Few recent examples of cyber attacks to IoT infrastructures and data breaches are:

- the Verkada breach[2], where a group of cybercriminal succeeded to access and control thousands of security cameras, accessing also at video footage of clients stored on the cloud. Verkada was not aware of the breach until the discover of videos posted online.

- the SolarWinds supply chain attack[3], a sophisticated attack where the investigation

[1]https://ir.mcafee.com/news-releases/news-release-details/new-mcafee-report-estimates-global-cybercrime-losses-exceed-1

[2]https://www.verkada.com/security-update/report/

[3]https://www.cisecurity.org/solarwinds

is still ongoing.

- the BotenaGo malware[4] that infecteed millions of router and IoT devices from Netgear and D-Link.

- the EasyJet attack[5] that exposed around 9 millioon email addresses and travel details of customers.

The National Security Agency (NSA) established the "Science of Security"[6], an initiative to improve scientific research in the field of cybersecurity, that lead to the creation of the Five Hard Problems (5HP) of cybersecurity. This provide a structure to the problem and encourage collaboration across disciplines. The problems discovered were:

1. **Scalability and composability**: when dealing with large systems, components integrate to form a new larger system: other than increasing the amount of possible attacking point, it creates a situation where the risk related to each individual component may not directly translate into total system risk.

2. **Policy-governed secure collaboration**: Effective and well-defined policy are fundamental to develop recommendations and guidelines to promote the secure operation of systems, to enforce normative requirements and standards and to handle authorities and permissions.

3. **Security-Metrics–Driven Evaluation, Design, Development, and Deployment**: This comprehends probability models for evaluating an attack, measuring the extent to which various security properties are present in a system, formalizing the analysis of systems.

4. **Resilient Architectures**: Despite of being under attack, systems should be robust to withstand attack, continue to provide services, restore functions, recover and minimize the impact.

[4]https://www.iotworldtoday.com/2021/11/16/botenago-malware-targets-millions-of-iot-devices/
[5]https://www.ncsc.gov.uk/news/easyjet-incident
[6]https://cps-vo.org/group/SoS/about

5. **Understanding and Accounting for Human behavior**: Finally, addressing the ways humans interact with the digital world: systems may be built with security measures, but those measures may be compromised by human behavior, accidentally or intentionally. Research in this field are on: identifying dangerous actions, examining the impact of social and cognitive factors of phishing scams, processing biometrics to distinguish between normal and malicious users, using persuasion research to quantify the likelihood of falling victim to phishing emails and so on.

As we can see, this is a multifaceted problem, and it's essential that a fundamental property should be addressed during and after the development of hardware and software: **security**.

Strategies and countermeasures such as Firewall, Antivirus, Intrusion Detection Systems (IDS), SIEM, etc.. are example that could be taken, but how can we understand when a certain level of security is achieved? How can we know if security policies and mechanisms are working and efficiently? If security is a property that is essential to have, we need a way to measure it.

Giving a simple answer to "How secure is this device/software/system?" is not obvious and it depends on many security factors, especially on the incomplete knowledge about the current situation: we don't know if some products hide vulnerabilities that even manufacturers still don't know their existence. Moreover, there is not a standardized way to classify products on their security level: we lack an unified view. Security metrics could be a tool that help to solve this problem: their purpose is to define a replicable way to measure how much certain security constraint are met, by analyzing aggregate data overtime. They can be seen as a group of questions that assign a resulting value depending on the answers, an example is shown in Fig. 1.1.

Reaching standardized security metrics is an ambitious initiative introduced in Europe [66] that opens new questions on which properties of systems to consider and which approach is able to address the complexity of the problem. Some frameworks that use

- **Description**: Measure of entropy in user space memory which quantitatively considers an adversary's ability to leverage low entropy regions of memory via absolute and dynamic inter-section connections
- **Results**: *Ordinal*
- **Scope**: *Software*
- **Automation**: *Automatic*
- **Measurement**: *Dynamic*

Figure 1.1: An example Security Metric from [6] with values for classification

security metrics are already available and they consist of questions that receive different types of answers. The context where they are applied can vary a lot, and a specific metrics could be not transferable in some scenarios [6], so a way to classify the type of metrics is needed for catalog them over the values of different properties, such as the one used in [6]:

- *Results*: the given result can be nominal, ordinal, interval, ratio, absolute, distribution.
- *Scope*: the metric can be focused on users, software, hardware, network, organization.
- *Automation*: the metric could compute results in an automatic way or it may need some manual work.
- *Measurement*: the computation of results can be static or dynamic, if the analysis needs continuous realtime recalculation.

Still, more criteria that reach different taxonomies could be created for every specific application such as in [42] where a particular taxonomy is built for Embedded Systems.

Different context requires different metrics and classification: in the next sections I introduce Cyber-Physical System and the reason why they are an interesting context for the applications of security metrics, as exposed in the first paper that I produce while working on this thesis [31].

Chapter 2

State of the Art on Security Metrics

Reference texts that deal with defining and standardizing metrics for measuring security in an IT context are ISO 27004 [12] and NIST 800-55 [19]. These documents suggest standard approaches to define guidelines for evaluating the performance of information security and efficiency of a management system aimed at meeting the requirements of the ISO 27001, defining what to monitor and how to do measures, with also a wide range of examples. The latter follows the same principle, trying to offer guidelines to follow for companies. The focus of these standards is on policies and processes, rather than to systems in general with their countless factors that influence the security state.

In [54] the methodology used to write those documents is criticized. Contextualization and alignment with business objectives is considered to be lacking, thus a new goal-driven strategy is proposed. The outlined solution seems to provide more accurate and appropriate results, but with a downside of requiring a huge effort for developing a clear and traceable relationship between metrics and business objectives that can lead to make the process of evaluation laborious.

Metrics, also, needs to follow some quality requirements. A way of evaluating a metric is described in [5] and takes into account:

- the measurability of properties that need to be consistently available
- the cost and the possibility to automate the gather of consistent data

- the way of distilling it in a quantitative way (e.g. cardinal number, percentage, ..)
- the definition of units

Still, in [5] the metrics proposed mainly deals with system properties, leaving the behaviour of the user and other factors mostly uncovered.

Some works analyzed specific fields in depth, such as [68] which focuses on network security metrics showing pros and cons of each one, while others performed surveys, such as [52], which compares many existing proposals regarding system security, measuring the effectiveness of security metrics on vulnerabilities, attacks severity and power of defense mechanisms. The conclusions highlight the existence of significant gaps between the available research results and the desirable metric properties. Such properties are sometimes defined with enough clarity for specific sub-fields, as it happens for security conformance metrics for managing industrial automation control systems in the [35] standard [35] that includes what characteristic a good metric should have.

Another deep but specific work covers the field of embedded systems (ES). In [42] more than 500 metrics were filtrated to match ES applications: 169 were selected and evaluated using SMART [22] and PRAGMATIC [17] criteria and characteristics identified in [59], basically measuring the comparability, cost effectiveness, measurability, repeatability and reproducibility of each metric.

Security metrics can also differ between apparently similar devices, for example Traditional Biometric Systems (TBS) and Wearable Biometric Systems (WBS); the dimension of threat and vulnerabilities change as illustrated in [64], in which the need of different metrics is motivated.

The discussion about security metrics that comprehend policies as well as technologies is lively also in an online community that organize a yearly scheduled conference[1].

[1] securitymetrics.org

As done in this survey [52] security metrics can be categorized on their scope: vulnerability, defense, attack and situation. I will present that categorization, where some example metrics are shown.

2.1 Vulnerability Metrics

These metrics refers to measuring a level of system vulnerability that depends on: user vulnerabilities, interface-induced vulnerabilities, and software vulnerabilities.

User vulnerabilities

User vulnerabilities can depends on users cognitive bias (e.g. susceptibility to phishing attacks) and cognitive limitation (e.g. weak passwords), so metrics can measure:

- *Phishing susceptibility*, with the percentage of false positive, i.e. genuine email flagged as phishing, and false negatives, i.e. phishing email flagged as genuine.
- *Malware susceptibility*, related to a user's online behavior such as installing many applications, visiting many websites, etc..
- *Password vulnerabilities*, evaluating the entropy and guessability. There should be an effort to derive an accurate result based on multiple diagnosed results from different metrics so a unified metric can represent a valid quality of a given password.

Interface-Induced vulnerabilities

Software interfaces typically contains receiving point for entering data that are used by attackers to inject malicious data. This is harmful if input data is not well sanitized, and can alter the normal functioning of the system.

Metrics can measure the attack surface, the sanitizing efficacy and usability of the interface.

Software vulnerabilities

Software vulnerabilities can be categorized as:

- **Temporal attributes vulnerabilities**, where metrics measure the evolution of vulnerabilities, such as the frequency of the presence or exploiting of that specific vulnerability, and the vulnerability lifetime, so how long does it take to patch the vulnerability since its disclosure
- **Individual software vulnerabilities**, where metrics measure software vulnerabilities with an emphasis on ranking them in terms of dangerousness. An example is CVSS, described below.
- **Collective vulnerabilities**: since many attack involve the use of more than one vulnerability, those metrics measure the dangerousness of the combination of vulnerabilities using attack graphs, Bayesian Network, attack tress and privilege trees.

The Common Vulnerability Scoring System (CVSS) is a published standard and open framework that "provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity"[2]. The calculator is available in the website. It is recently evolved from version 2.0 to 3.1, as shown in 2.1. It consist of three metric groups:

1. *Base metrics*, that produce a score ranging from 0 to 10 and can be then modified by the other two metrics. They represent qualities intrinsic to a vulnerability, such as the skills required to exploting it, if it is local or remote, what is the impact on CIA properties.
2. *Temporal metrics*, that can change over the lifetime of the vulnerability, depending on exploits that are developed, disclosed and automated and if remediation and patches are available.

[2]https://www.first.org/cvss/

3. *Environmental metrics*, that evaluates the severity of the vulnerability in its context, like the impact on physical and financial assets. Those metrics are subjective and so typically calculated by affected parties.

Metric	Definition	Scale
Base metrics: Exploitability		
Attack vector	Describes whether a vulnerability can be exploited remotely, adjacently, locally, or physically (i.e., attacker must have physical access to the computer)	Nominal
Attack complexity	Describes the conditions that must hold before an attacker can exploit the vulnerability, such as low or high	Ordinal
Privilege required	Describes the level of privileges that an attacker must have in order to exploit a vulnerability, such as none, low, or high	Ordinal
User interaction	Describes whether the exploitation of a vulnerability requires the participation of a user (other than the attacker), such as none or required.	Nominal
Authorization scope	Describes whether or not a vulnerability has an impact on resources beyond its privileges (e.g., sandbox or virtual machine), such as *unchanged* or *changed*	Nominal
Base metrics: Impact		
Impact metrics	The impact of a successful exploitation of a vulnerability in terms of confidentiality, integrity, and availability, such as *none, low, high*	Ordinal
Temporal metrics		
Exploit code maturity	The likelihood a vulnerability can be attacked based on the current exploitation techniques, such as *undefined, unproven, proof-of-concept, functional, or high*	Ordinal
Remediation level	Describes whether or not a remediation method is available for a given vulnerability, such as *undefined, unavailable, workaround, temporary fix, or official fix*	Nominal
Report confidence	Measures the level of confidence for a given vulnerability as well as known technical details, such as *unknown, reasonable, or confirmed*	Nominal
Environmental metrics		
Security requirement	Describes environment-dependent security requirements in terms of confidentiality, integrity, and availability, such as not *defined, low, medium, or high*.	Nominal
Modified base	Base metrics customized to a specific environment	*

Figure 2.1: CVSS, as in version 3 [52]

CVSS can be used in conjunction with the Common Vulnerabilities Enumeration (CVE)[3] for identification of vulnerabilities and their CVSS score, as proposed in *https://www.cvede*

[3]https://cve.mitre.org

2.2 Defense metrics

These metrics measure the strength and the effort needed for placing in a system defense mechanisms.

Preventive defenses

These defenses act before attacks and aim to block them. For example, metrics can measure:

- the strength of *Blacklisting*, as the delay needed between the observation of the malicious entity and the block of it (reaction time), or as the portion of blacklisted malicious entities (coverage)
- the effectiveness of *Data Execution Prevention* (DEP), that tries to avoid code injection that requires the presence of a memory region both executable and writable by excluding in time the two actions.
- the quality of *Control-Flow Integrity* (CFI), that try to mitigate attacks based on memory corruption. Metrics can measure the reduction of number of targets exploitable, the average size of targets, the evasion resistance.

Reactive and proactive defenses

These defenses detect malicious actions and act to interrupt them (e.g. Intrusion detection systems or IDSs). They can measure the strength of:

- **Monitoring**, calculating the coverage, the amount of redundancy sensors or information, the confidence in which sensors still detect correctly events if some of them are compromised, the cost in terms of resources consumed by deploying sensors and mantaining them
- **Detection**, calculating the detection time as the delay between the time in which system is compromised and the time of discover of the attack, the confidence in

which an alarm is related to a real danger, the IDS statistics (e.g. TP/TN/FP/FN rate, costs, capabilities,..), etc..

- **Proactive defenses**, evaluating the efficacy of such mechanisms, such as Address Space Layout randomization (ASLR) by measuring the entropy of a memory section or Moving Target Defenses (MTD), that will be better explored in Cap. 3.4
- **Overall defenses**, with penetration testing techniques or attack graphs that estimates the effort required to compromise the system.

2.3 Attack metrics

These metrics measure the strength of attacks performed against a system.

Zero-Day attacks

To quantify the strength of zero-day attacks metrics can measure, based on past activities, the **period of time** between the launch of an attack and the public disclosure of the vulnerability or the n**umber of devices compromised** in remote zero-day attacks.

Botnets

Botnets are groups of devices that are connected to the Internet and each of them runs one or more bots that can be used to perform Distributed DOS attacks. Metrics can measure the **size** of the botnet as the number or bots that compose it, the **network bandwidth** that a botnet can use to launch DOS attacks, the **efficiency** as the network diameter of the botnet topology, the **robustness** of botnets under random or intelligent disruptions.

Attack evasion techniques

Attacks try to evade defense mechanisms in different ways, the strength of such techniques can be measure by metrics that evaluates the use of **Adversarial Machine Learning Attack**s or the type of **Obfuscation**, that is done by a set of tools (e.g. runtime packers) widely used by malware creators, to avoid static analysis. Metrics can measure the occurrence of obfuscation in malware samples or the runtime complexity of packers measured in the numbers of layers or granularity.

2.4 Situation metrics

These metrics measure the complete management of attack-defense interactions in relation to information system, depending on a certain time *t*.

Security State

The security state of a system depends on the moment of analysis because it dynamically evolves from time to time as the outcome of attack-defense interactions. Metrics can be **Data-Driven** measuring:

- the **Network maliciousness**, as the estimation of the fraction of blacklisted IP addresses in the network
- the **population** of networks used to launch drive-by download or phishing attacks and the effect of spam from one ISP or Autonomous System (AS) on the rest of the Internet
- the **Control-plane reputation**, evaluating the maliciousness of attacker-owned ASs based on their control plan information (r.g. routing behavior)
- the **Cybersecurity posture**, that is the aggressiveness of attacks measured as the dynamic threat imposed by the attacking devices (e.g. attacks observed at honeypot)

or **Model-Driven**, measuring:

- the **Fraction** of compromised computers
- the **Probability** that a computer is compromised at time t

Security Incidents

Another aspect of the security of a system at a specific time t is give by the past security incident that the system experienced. Metrics can measure:

- The **frequency** of incidents as: the rate of encountering malwares or being successfully infected, the rate of successful countermeasures, or even the time between incidents or time between the starts of a device and when its first malware alarm is triggered.
- The **damage** of incidents as: the **delay** in detection and remediation, the **costs** in terms of direct (e.g. money loss) and indirect costs (e.g. reputation, recovery costs). Those estimation needs to be accurate to give a meaningful result.

Security Investment

Finally, to justify and encourage security investments, those efforts done by the company to ensure enterprise's security needs to be related also with economics. They can be measured as:

- the percentage of **IT budget**
- the quantity of **security budget**
- the reduction in the loss by improved security that is called **ROSI**, similar at the return on investment (ROI) metric
- the difference between the present economic value of future inflows and the present economic value of outflows with respect to an investment

2.5 Discussion over the actual security metrics literature situation

To achieve **completeness** of security metrics, it is unavoidable to deal with a tradeoff issue between dimensions of data and accuracy. That is, how to reflect the completeness of attributes measured in metrics explains the part of why developing good metrics is a hard problem. A possible solution is to build metrics that rely over a simplified but still accurate model that represents the threat environment, allowing to employ tailored defenses.

The **uncertainty** present in the security field makes security metrics difficult to measure: attack behaviors are hard to be accurately predicted and can be unknown (e.g. zero-day vulnerabilities are not prevedible) and some estimation errors can be present if we have detection errors and human cognitive limitations. It would be ideal to measure the intuitive metric of users' susceptibility to attacks based on the social sphere, depending on personality or biases of people.

It should be reached a tradeoff also in the extent of **aggregations** of metrics, because even if the granurality obtained in having so many different metrics can give more detailed information, it would be endless to report all the details of that security situation.

There is the lack of a set of **standardized** metrics or even a standardized classification: those are the next step that needs some research effort to reach more practically usable metrics.

Chapter 3

Applications of Security Metrics

Context of application of security metrics can vary a lot: metrics could be focused on company's policies, (e.g. access regulations, password managements, ...), software development (e.g. secure coding, vulnerabilities, ..), network security (e.g. insicure interactions, correct use of firewalls, ...) and more. So, as said before, every one of those contexts need specific developed metrics that could be not transferable to other situations.

In this section some of the applications of security metrics are proposed, with the intention to show practical example in the use of them, the results obtained and the strategies or methodologies used to select those specific metrics.

3.1 Software life cycle

Starting from the beginning, Software should be developed with the "Secure by Design" approach in mind that is essential to reach more secure product[1] instead of measuring security in its absence[2]. Security should be a property to be met since the development of software because it's been observed that over 90% of vulnerabilities occur as a result of flaws in that phase [67].

[1] http://www.networkmagazineindia.com/200610/vendorvoice02.shtml
[2] http://www.safecode.org

However, software development is a complex task and comprehends different phases, from the initial design and development to the implementation, testing and update. To help the developers keeping track of security requirements in every phase, metrics can show the results of various analysis for early detection and correction of vulnerabilities.

In literature, proposed metrics have been there for a while, resulting in at least 324 unique metrics [48] that spans from the analysis of the product itself to the processes to develop it.

However, various reasons demonstrate that is not easy to provide useful metrics, for example: the difficulty in creating effective models for security risk, the dependability on psycological factors of software developers, users and attackers and also the delay in seeing security problems only when the product is finished or used by consumers.

So, even though the number of metrics found by the study is over 300, the ones to be used in a single project development should be carefully selected, limiting them to be not more than 20 to keep the project manageable[3], that's why classifying them is essential as a guideline to create a subset of metrics that cover every aspect.

The majority of metrics available that apply to the software life cycle production consider:

- the achievement of **security properties** (e.g. Confidentiality, Integrity, Availability) and security requirements from the project.
- the **project management** strategies, analyzing the planning and the processes (e.g. the coverage of the security functionalities examined during verification).
- **resources**, like people, costs or time, that are computed as the effort needed in the course of security attacks or defends (e.g. number of developers that touched a binary and have left the company) .

[3]http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7564.pdf

- **vulnerabilities** of the products, that can be find with different strategies: CVE counts from public vulnerability databases, from public vendor vulnerability databases, from privates, from the development team, from analysis tools, using CVSS to rank them. Those are the most used and cited metrics in literature [48].

- the **defensibility** level of the product, so how it's easy to have a successful attack and how the product can react to recover (e.g. measuring the attack surface as the subset of its resources that an attacker can use).

This way, metrics try to cover how security is assessed during every phase of the product development [63] (e.g. Ratio of omitted security requirements, number of security algorithms, ratio of patches,..).

Resulting applications

To understand how much security properties are implemented in software, metrics based on the achievement of security properties can be used to quantify them.
Metrics based on project management strategies can ensure quality achievement assessing the development process.
Developers and other stakeholders can assign economic values to the risks of the software using metrics that consider resources.
Metrics based on vulnerabilities, instead, can give a direct measure of the risks derived from the use of the software.
Finally, in the design and implementation phases, metrics that consider defensibility can be used as a direct measure of risks associated.

3.2 Control Systems

Control systems has evolved since their beginning and, thanks to control theory, now they can show robustness against disturbances. However, the presence of adversarial disturbances changes everything and the occurrence of successful attacks to them is increasing.

Typical countermeasures against attacks to control systems are based on fault detection: they try to forecast the evolution of the system and, if the real system's behaviour differ more than a predefined amount, it raise an alert.

In case of stealthy attacks, i.e. where the attacker try to hide himself, the threshold may never be reached and fault detection could not be enough. [49] presents two type of security metrics that can be used as tools to quantify and minimize the impact of the attacks. Given the set of the states that stealthy attacks could induce in the system:

- the first metric consider the size of this set for every different subsets of sensors of the control system, giving the possibility to measure the sensitivity to attacks for particular sensor or combination of them.
- the second metric, that add priority to particular states, consider the minimum distance from the attacker's reachable states to critical states that could produce worst outcomes if exploited.

The results given from the mathematical analysis of those security metrics provide synthesis tools to redesign controllers, fault detectors and monitors minimizing the impact of stealthy attacks, as shown in [49].

The more different types of metrics are available, the more we can provide security insight of the system from different perspective. [11] proposes a framework for developing security metrics for industrial control environment by defining the target, defining the objective and finally synthesizing the metrics. The framework tends to unify existing security metrics development approaches, methodologies and guidelines with the improvement of adaptability. The steps are:

- **Target Definition**: In this step, the goal is to delineates attributes of the system or environment for which security metrics are being generated, by defining
  - the capability of the system to uphold a protected state and the flip side of it, i.e. vulnerability, that is the inability to achieve or sustain a protected state
  - the section of the system for which security perspectives are desired, comprehending machines, network connections, software, functionalities, configurations.
  - the constituent of the segment that the framework has to focus on: people, process and technology.
- **Objective Definition**: To generate goal-oriented metrics that provides information that shows the attainment of predefined security objectives, the framework require to know
  - primary and secondary objectives, such as availability, integrity, confidentiality and safety, that in the ICS domain should be included for the preservaton of injury and damage to people and systems.
  - the analysis of violation concepts and a contextual description of the desired state of security objective.
- **Metric Synthesis**: Finally, defining the dimensions of the metrics with their quantities and specifications.

The framework has been validated with a two-level approach: an use case scenario on human capability evaluation and a questionnaire to experts on security metrics generation. The validation results in relevance, reliability, and practicality of the framework that depends on the precision of the first two phases: **the outcome of a security metric development will be determined by the clear and concise articulation of system scope and target security objectives.**

3.3 Evaluating Electronic Health Records Systems

The electronic health record (EHR) is a digital and institutional document that represents all the records of patient care from different domain (e.g. demographics, allergies, ...) so it contains a lot of patients sensible information that has to stay confidential. Transitioning from a paper-based document to the digital world improve costs, quality of care, record keeping and more[24], but it comes with some privacy and security threats that regulation try to overcome but it still end up in some successful attacks costs totaling 9 million of dollars in 2021[4].

Security metrics find application in this domain and [44] demonstrates that by exploring academic and grey literature to collect metrics to be used for evaluating the quality of security of EHR. The method chosen to select the security metrics was to follow the guidelines to conduct a Multivocal Literature Review (MLR) [28], benefiting from the inclusion of grey literature, gaining information in areas such as Software Engineering and closing the gap between academic research and professional practice.

MLR is based on:

1. the parallel study search on academic and grey literature that evolves in the selection of the studies
2. the filter of the most promising ones
3. the merge with other studies thanks to the snowballing process [72]
4. the final extraction of selected studies, done by following some inclusion and exclusion criteria (e.g. include if the study is directly related with security metrics, exclude if it's shorter than three pages).

The study ends up with 19 metrics that covers 5 different security areas: Confidentiality (4), Work-space security (2), Integrity (2), Availability (3), Security management (8).

[4]https://www.hhs.gov/sites/default/files/2022-02-17-1300-emr-in-healthcare-tlpwhite.pdf

Totally satisfied	The EHR system has a plan and policies to manage the data in case it is lost. The plans and policies **involve** the following steps: • Identification of sensitive EHR data • Knowing where the data is and who has access to it • Classification of data in terms of importance and potential damage to the EHR system • Identify who owns the data • Regulation of data owners' liability • Determine whether certain data are necessary or obsolete • Deletion of data as soon as it is no longer needed
Satisfied	The EHR system has a plan and policies to manage the data in case it is lost. Nevertheless, the plans and policies **partially** involve the following steps: • Identification of sensitive EHR data • Knowing where the data is and who has access to it • Classification of data in terms of importance and potential damage to the EHR system • Identify who owns the data • Regulation of data owners' liability • Determine whether certain data are necessary or obsolete • Deletion of data as soon as it is no longer needed
Neutral	There are **undefined** and **informal** procedures for recovering lost data (for example, calling someone in case some data is missing or does not arrive).
Unsatisfied	A procedure for handling lost data exists, but it is not possible to **establish** and/or **evaluate** the details of such a procedure.
Totally unsatisfied	No control or management of lost data exists.

Figure 3.1: Example metric from the Integrity area called "Management of Lost Data" [44]

The metrics has results values that ranges from 1.0 (Very insufficient), 2.0 (Insufficient), 3.0 (Sufficient) to 4.0 (Very sufficient), associating with every level a description that shows how a value is assigned, an example is proposed in Fig. 3.1.

To validate the set of metrics an use case is presented [44], where medical information of 2 million patients where violeted and exposed online. The study gather, after an agreeement of anonymity, the roles of the actors that where implicated in the cyber attack, and each actor evaluates, and discuss on the reason of the choice, each metric following a Likert Scale: Totally effective, Effective, Neutral, Not effective and Totally not effective. The majority of the results where on Very effective and effective, with final comments from the participant that the selected set of metrics would have been effective in mitigating the security incident.

3.4 Measuring the effectiveness of Moving Target Defense techniques

The shift from static networks, based on hardware, to dynamic programmable software-based networks that is happening with emerging networking technologies (e.g. SDN) calls for a novel and proactive defense mechanisms: Moving Target Defense (MTD).

MTD is based on adding uncertainty and complexity into the system, continuously changing the attack surface of it, to make it difficult for attackers to identify vulnerable components and exploit vulnerabilities. Since there is a large number of proposed MTD techniques, it will be essential to assess the effectiveness of them to select the ones to deploy.

Comparing different MTD's techniques involves:

- Understanding if the new states that the network reaches after MTD is triggered are effective in thwarting the threats
- Evaluating pros and cons of the new attack surface that is generated between the states, to understand whether it is worth it

To consider those two aspect [36] propose newly developed dynamic security metrics based on attack and defense efforts.

- **Attack efforts metrics**: by evaluating the quantities, the duration and the costs of possible attack paths as the network change states: the less they are, the more is difficult for the attacker to succeed.
- **Defense efforts metrics**: by evaluating the resources required, the time to shift to the other state (that could include downtime of the system), the overhead introduced: the less they are, the more we save useless efforts.

The study demonstrates the use of those metrics over Software Defined Network (SDN) and do a comparative analysis via simulations to assess the effectiveness of MTD

techniques, comparing them to the choice of the chosen metrics.

Those simulations demonstrates the usability as well as effectiveness of the security metrics approach: the results showed that is possible to find a trade-off between the attack and defense efforts, as increasing the attack efforts also increases the defense efforts (i.e., reducing the security risk increases the security cost) thanks to the in-depth details given by security metrics.

3.5 Applications overview

Other applications of security metrics are:

- to measure the security in vehicular systems [26].
- based on the Goal Question Metric approach, to improve misuse case modeling in system development [Security Metrics To Improve Misuse Case Model].
- their dynamic calculation to help on the selection of countermeasures to take against network attack [Selection of countermeasures against network attacks based on dynamical calculation of security metrics]
- to create an executable state-based security model of a system and an adversary that represents how the adversary is likely to attack the system and the results of such an attack [40]

As seen, using security metrics requires to gather data, calculate estimations and run simulations, all operations that sometimes can be energy demanding. So, to limit the needs of computational resources, the set of metrics need to be reduced to the bare minimum, trying to cover the same every aspect of security.

It's important to notice that the selection or creation of security metrics for specific application needs some preliminary work. As we saw, more approaches can be followed:

1. **Classification and selection**: this is the approach followed in 3.1, it needs to define a classification for the metrics that is coherent with the domain and then selecting them to cover all the security aspect that are required
2. **Automatic generation**: as in 3.2, it needs a framework capable of generating specific security metrics and a preliminary study that analyze the context and the security objectives of that field.
3. **MLR**: used in 3.3, by exploring the academic and grey literature, using the snowballing process and filtering them with a multi-step approach.

Those methodologies can be used, separately or combined together, to create a set of security metrics in different domains, but require a lot of manual work to be applied.

3.5.1 A.I. for generating metrics

Due to the amount of metrics available, the three methods presented require time and labor to select them. The question then arises whether this work can be automated. This is where A.I., or at least a specific area of it, comes in.

Let us take the example of multi-level neural networks, as shown in Fig. 3.2. They have a set of hidden layers, which form the black box of the system, that adjust their weights following the rules of machine learning. Neural networks are complex systems that achieve high rates of accuracy, which is why they have been much explored and used in recent years. However, they suffer from a serious problem: the decisions made by these networks are not fully explainable. We can say that they have learned, from the initial data set, to classify samples, but we cannot know the exact reason for certain choices.

In the security field, this type of A.I. can also achieve good accuracy, but since it cannot explain why a certain sample was considered malicious or not, its usefulness is questionable.

The **explainability** is important in the field of security, which is why techniques such as Decision Tree may find more interesting applications. Decision trees, unlike neural networks, have a simpler operation, they work by building a decision tree composed of nodes that separate, according to the meeting of certain criteria, the dataset into different portions. It is important that the criteria within the nodes are chosen correctly, and there are algorithms to optimize their arrangement so as to obtain better classifications.

In essence, tree-based methods and neural networks can be put in the same category as the way they approach problems is by deconstructing them piece-by-piece, instead of finding one complex boundary that can separate the entire database. The key difference is that decision trees can show step by step why a certain decision was made and what

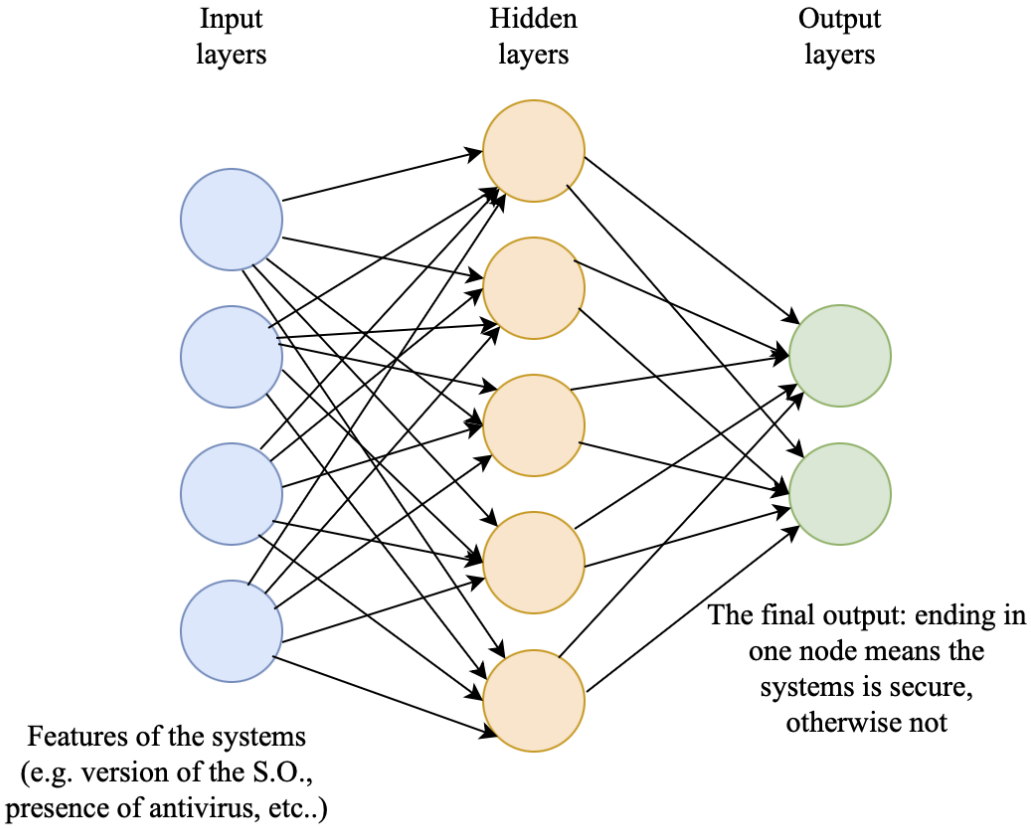

Figure 3.2: Example of a neural network with one hidden layer to classify if a system is secure or not.

features defined it in a certain way. Let's take the example of Decision Tree built to classify the security of a system, as the one in Fig. 3.3. The tree is composed, node by node, by conditions that results to make the system secure or not. Those can be take as security metrics, automatically generated with already some assurance on their efficacy, since it works on the dataset. So Decision Tree could be used to:

- **generate security metrics**, by taking the feature selection of the tree.
- in an opposite way of the first point, **evaluate the security of systems**, placing the security metrics already selected via other methods (e.g. MLR) as the feature selection of the nodes of the tree.

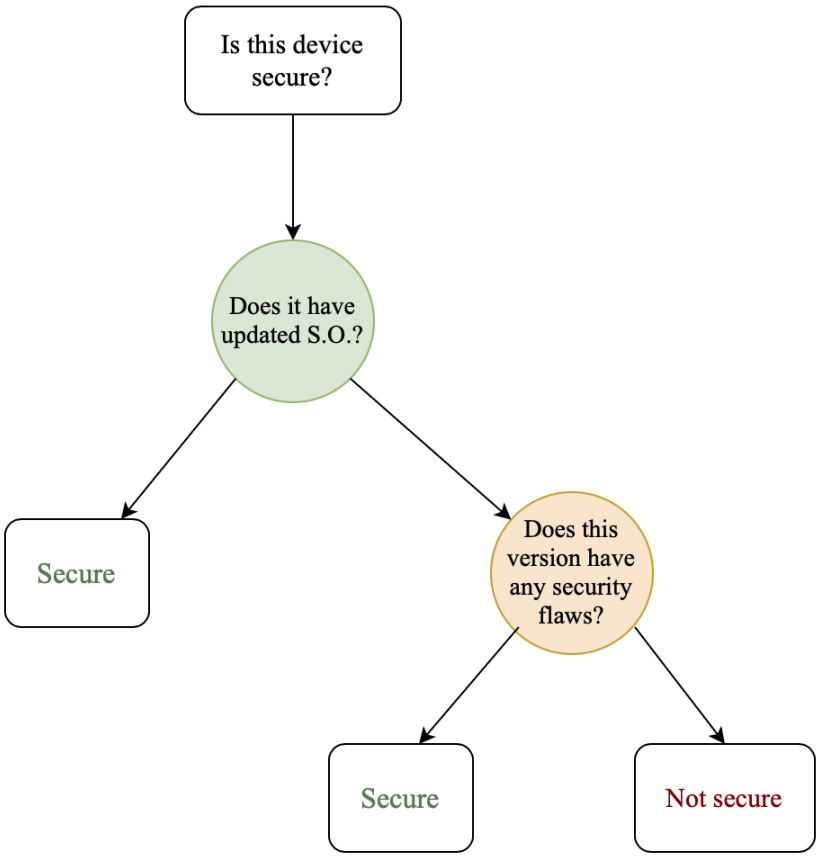

Figure 3.3: Example of a Decision tree with only two nodes to classify if a device is secure or not. The questions in the nodes can be taken as security metrics.

As it seems very simple, this technique still hides an important requirement: **the dataset**. It's not that easy to choose the critical security feature of systems and find example of secure or not secure system correctly categorized with all their characteristics, especially if they have to be very similar to the one to find security metrics, and still some manual work should be done for that.

At this moment in literature is not present any in-depth study on this topic, therefore

I argue that it could be an interesting possibility for generating security metrics which should not be discarded a priori because of its automation possibilities.

Chapter 4

Security metrics and Cyber-Physical System

A picture emerges from the short overview we provided in the previous sections. Some frameworks for measuring security properties exist, applications are at their early stage but seems to provide encouraging results on security improvement. However they leave many gaps open, especially in terms of inter-disciplinarity. Comparative analyses and reviews sustain diverging opinions regarding the suitable approaches to take on metric definitions and applications.

It is evident, however, that there is a drive to tackle these issues at all levels, as proven by the inclusion of the topic in the European Union's Cybersecurity Act [66]. Given these premises, it is interesting to reason and investigate on the current application of the security metrics in Cyber-Physical Systems (CPS) and on the consequences of having a such standardized view on evaluating security of systems.

4.1 Cyber-Physical Systems

Cyber-Physical Systems "integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other" and are at the center of current research and innovation activities [6]. They are ubiq-

uitous, involving spheres not limited to production activities, but also contexts directly affecting human well-being such as transports, environment, and health.

CPS are interconnected with the concept of Industry 4.0 that is the process of combining technologies (e.g. Bid Data, Cloud computing, IoT, ..) and knowledge, providing autonomy, reliability, and control without human participation.

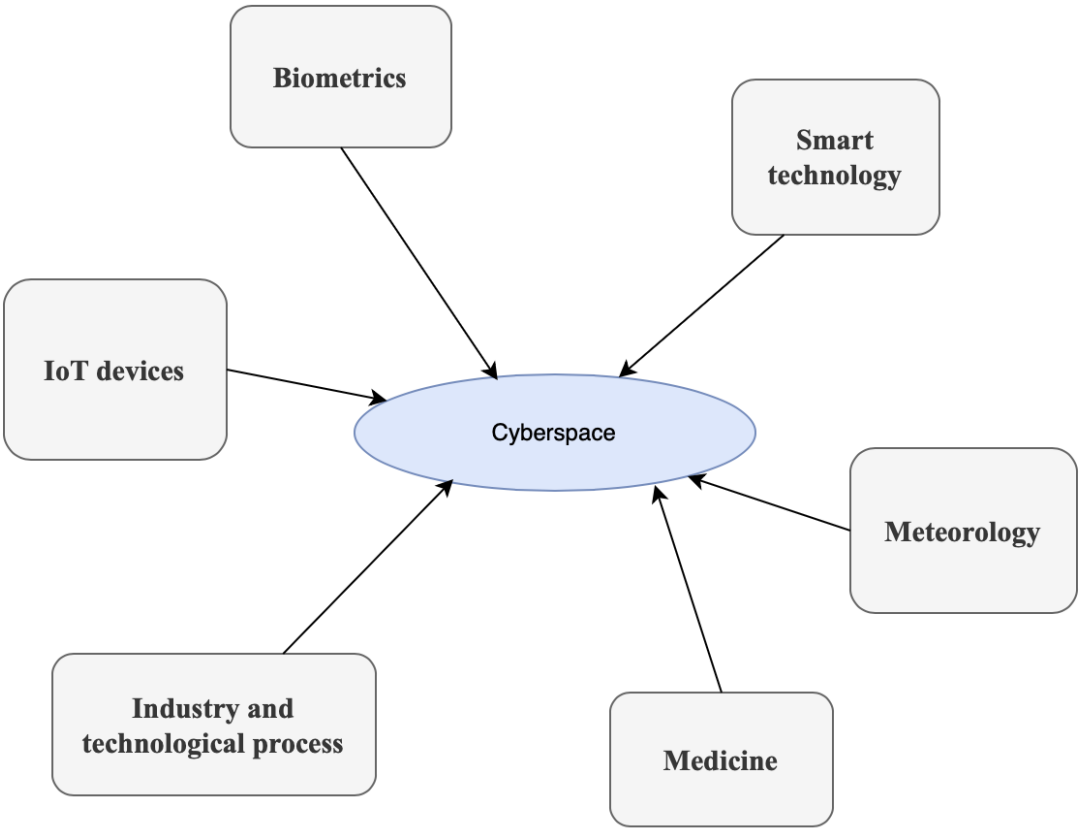

Figure 4.1: CPS components

A substantial difference with the Embedded Systems is that in CPS is present the integration of cybernetic, computer hardware and software technologies that are embedded in their environment and able to perceive its changes, learning, responding and adapting to them.

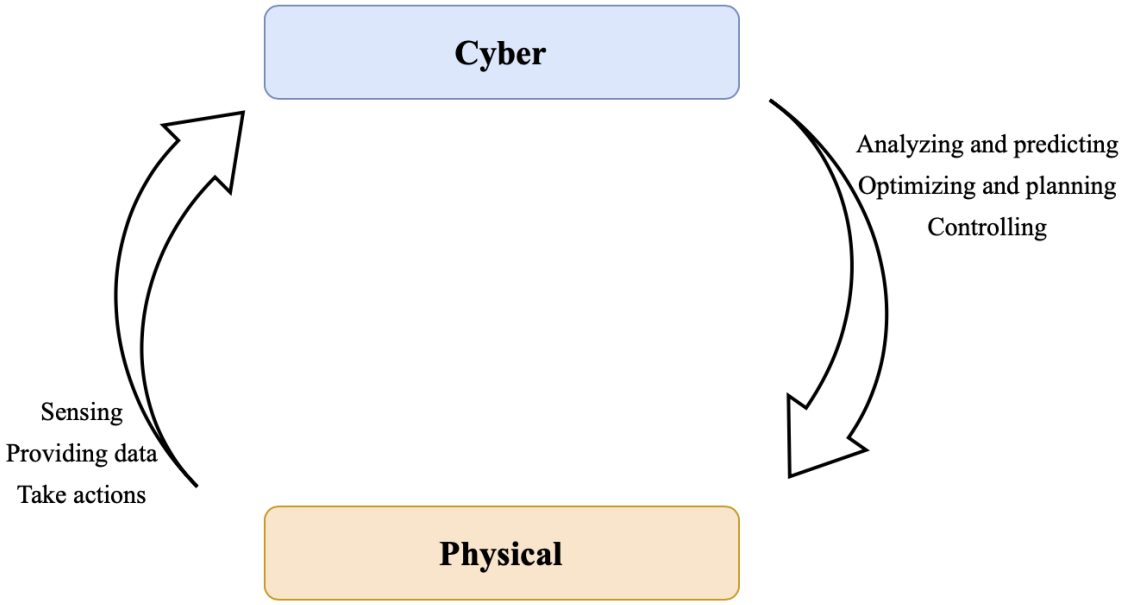

Figure 4.2: Cyber and Physical interactions in CPS

CPS include computing and physical processes, with the presence of a common cyberspace that provides exchange from systems and environment,as shown in 4.1. We can see them as consisting of two layers:

- The Physical part, with sensors and actuators that provide data and take actions
- The Cyber part that adapt, learn, make decisions and previsions for controlling the other layer.

Their complexity calls for an increasing adoption of automation, both in terms of intelligent, autonomic operation of single subsystems, and of their orchestration at the infrastructural level. Algorithms drive the activation and configuration of components, as well as their interconnection and interaction with the physical world. The decisions take into account functional requirements, system and network parameters, and measurements from sensors. Security properties are not factored among these factors with the same effectiveness, essentially because their evaluation is hardly structured and objectively distilled in quantitative terms.

Furthermore, even when security properties are explicitly mentioned, e.g. as a part of safety standards, their scope is limited to narrow technical aspects. The effects of deploying and operating CPS, however, reach out to a wider spectrum of issues, including social aspects and the protection of fundamental human rights such as privacy, ethical concerns, physical safety, as well as the interaction with the surrounding scenario of threats and the need for integrating intelligence about them.

The humanitarian expertise of CPS realities and technologies and its bioethical support is a non-trivial task and requires complex interdisciplinary teams of developers, researchers, philosophers.

Threats to CPS includes spoofing identity, tampering with data, repudiation of origin, information disclosure, elevation of privilege, Denial of service (DOS). Key problems are:

- Understanding the threats and the possible consequences of attacks
- Determining the peculiar properties of CPS and the consequences that differs from traditional systems
- Finding and testing the security mechanisms applicable to CPS

In [31], we claim that to guarantee fundamental rights to safety of individuals, in a society facing the widespread adoption of cyber-physical systems, research should achieve a structured, formal modeling of security properties encompassing all of the relevant disciplines. The model should define metrics that can be practically implemented as a part of the automated operation of CPS, to assess the compliance of security properties with expected requirements, both in real time and as a prediction of the outcome of changes to come.

4.2 What is the status of application of these metrics in CPS?

Research works exist [7] that attempt to define security metrics specifically for CPS context. However, practical results are achieved by focusing on the specific elements of the systems, while not considering emerging properties of their composition.

The interest for a systematic approach towards security metrics in CPS can be found in recent works such as [6], in which a test is performed to assess how well the metrics being considered meet certain conditions. The results show coverage of almost all desired features, but no metric manages to completely cover all proposed challenges. The most critical gaps regards attack detection and the biggest concerns refer to the fact that the analyzed metrics focus on the specific elements of the systems, while not considering emerging properties of their composition. They do not consider, or partially consider, dependencies and side effects in System of Systems (SoS) contexts and mainly focus on vulnerabilities and attacks.

There are some initiatives, like the mentioned Cybersecurity Act [66], that have the goal of establishing a cybersecurity certification framework which could lead to standardized security metrics. The problem that they encountered are the fact that there is an high degree of heterogeneity of devices to be taken into account, and the context of application may change a lot [45]. Moreover, an agile certification process is required because vulnerabilities can increase over time and the evaluation should be up-to-date during the life-cycle of CPS.

The metrics should be efficient and cost-effective to make the evaluation rapid, both at design time to avoid delaying the introduction of innovations in the market, and at operations time to make the evaluation useful for deployment and reconfiguration purposes. The metrics should also strike a trade-off between the complexity of the analysis and the need to show an understandable result for end users.

The benchmarks defined in [6], once the limitations cited in the previous section are

known, could serve as a starting point for future security metric definitions for CPS.

Another regard considering the threat environment or not: attackers behaviour could be taken as a training field, getting more precise estimation of security or the amount of damage that a specific attack could produce. For example, if we compare two systems with the same vulnerability that, if exploited, could produce a relatively small damage in the first system but catastrophic in the second, can we say that one is more secure than the other? Should our metrics consider the impact of a possible attack? How to model the environment that metrics will consider? There is not a simple answer, but we argue that an approach could be to mix environmental depending metrics with the others, developing a model of the environment that considers the involvement of the digital, physical and social worlds.

4.3 What are the prospects for real application of metrics to CPS?

In CPS is not enough to evaluate single component separately but there's the need to evaluate the overall system, so the metrics should take into account the communication and collaboration that devices have with other component. There is also the need to use only the metrics that are applicable and meaningful for CPS.

In [45] more than 500 security metrics where analyzed to select the ones applicable in the Embedded Systems field and the result was that almost 1 in 5 of those metrics were applicable, and only 0.6% referred to hardware vulnerabilities, which is striking considering how important this aspect is in ES. A similar analysis should be done for CPS, and to make it possible there is the need to better understand the security issues that can affect a CPS environment and elaborate the correct metrics from that.

In [7] an example of theoretical framework of metrics for CPS is discussed, where metrics take into account the overall systems without focusing only on single components. Making these kind of evaluation takes more time than a simple vulnerabilities evaluation

and can lead to delaying a product into the market: so there's the need of finding a trade-off between complexity of the evaluation and timing/resource usage.

4.4 How can security metrics be integrated into CPS?

On the one hand, an efficient usage of metrics depends on the specific parameters that are measured and the subsystem that is affected. For example, metrics that evaluate the security of the network should be placed not only in end-device but also in devices composing the network in contrast as metrics that only evaluate software of end-devices.

On the other hand, the complexity of interactions calls for a more holistic propagation of information, that may prove relevant also in contexts that, at a first glance, could not appear directly involved. Threat evaluation and risk analysis are the starting points to build a model linking measurable parameters of the CPS with its features, components, and operational conditions.

The attack surface can change over time so the "security score", i.e. the output of the analysis, should be up-to-date. Where physical attributes are involved, e.g. printed QR codes that label components for asset management and for initialization of trust relationships, efficient ways should be devised to incorporate security checks on their validity. Freshness of checks must be enforced, as for example PKIs do by placing an expiration date in certificates.

In terms of vulnerabilities, a starting point could be the automated scan performed by already available tools like Nessus[1] or Nmap[2], to derive an aggregate score or even to specifically evaluate the impact in terms of Confidentiality, Integrity and Availability (CIA) the way CVSS do. Even if we keep considering only purely technical parameters, this kind of scoring could be inadequate, especially in critical systems where also the resilience of the system must be taken into account. This study [73] paper proposes a

[1]https://www.tenable.com/products/nessus
[2]https://nmap.org/

design for metrics to evaluate the resiliency of Cyber-Physical Energy Systems (CPES) against attacks, using fuzzy Choquet Integral, again showing the struggle that leads to sacrifice generality for applicability.

The basic problems with vulnerability assessment is that they perform a search that is not exhaustive and is only based in already known vulnerabilities.The common path taken to get more useful results involves red-teaming exercises, penetration testing drives, and other means of actively probing defences for weaknesses.

These tasks usually yield wider and deeper coverage of potential security issues, but require significant human interaction and cannot be easily automated. Moreover, the results could end up biasing the resulting measurement, depending on how many (and which) of the possible testing paths are taken through the system [61]. This issue has started attracting some attention, with papers proposing security metrics to guide ethical hacking activities towards more reliable results [8].

4.5 What effect might formalizing the security level have?

To understand some of the consequences of formalizing the security level, we need to learn more about the current users and consumers awareness about cybersecurity.

4.5.1 Consumer Awareness

Cybersecurity awareness depends on various factors, personality included [60], so it can vary a lot among heterogeneous consumers that could often trade security and privacy for convenience. One example of reactions to data breaches [50], shows that 51% of their respondents reported they “Changed password or PIN” after receiving the notification, from which 24% “Closed or Switched Account” and 24% “Became More Diligent”. The 22% “Took no Action”. The study shows that often customers are not aware of the

impact of the data breach, maybe due to the economic (ir)relevance of the account [3].

Another interesting work is [4], where a survey results in majority of people following bad practises such as personal information on passwords or opening unknown email or links. That lead to almost 80% of them being victim of phishing emails and infected by malware, changing behaviour and showing higher degree of concern only after the incident. On another survey [56], participants indicate theft as the bigger cyberthreats, whereas phishing and cyber stalking rely only in the minority (from 1 to 2%) even if expert suggest that one of the most important security vulnerabilities is inarguably phishing. Also, the majority thinks that the steps needed to protect their online security and privacy is too overwhelming to think about, even if 57% of them personally experienced a cyber-attack.

In [9], a survey is done that analyzes aspects of consumers experience with home IoT: participants express high concern about weak password and unsecured wifi password, desiring to have feature for more security, like an assistant for authentication, as shown in Fig 4.3.

Then, how would an increased security awareness from consumers affect the adoption of IoT technology? Traditionally it was believed that the more awareness, the less users are prone to the adoption, but work as [34] seems to show a weak, but not negative, impact on the rate of adoption of this technology. Instead, having users not aware of the problematic, with the majority of them not currently concerned and implicitly trust their devices, implies that only manufacturers can address such security issues.

Placing the burden of safety solely on manufacturers is not effective: there is no purely technical solution to make systems secure, and for these reasons user behaviour is still a critical attack vector. In [2] is reported that information security is heavily reliant on the behavior of individuals. Awareness is important, that's why we claim the necessity of a security culture in our organizations [20] and society that have to start from early education.

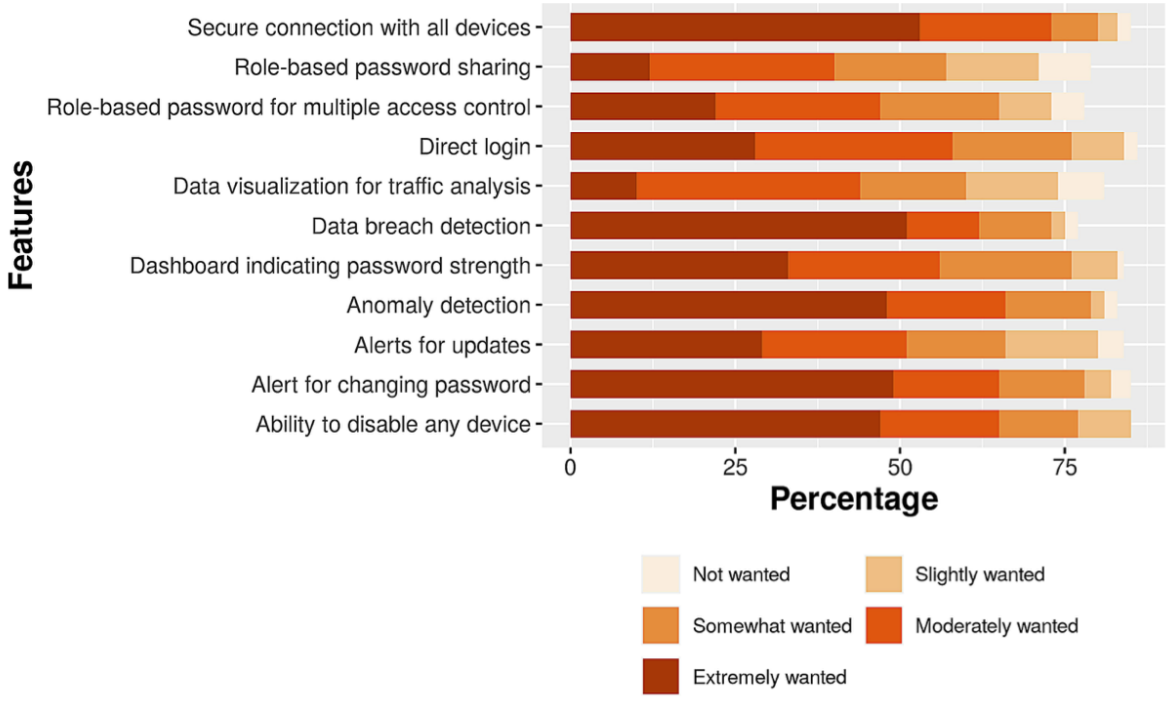

Figure 4.3: Liker scale responses for participants' preferences to secure features related to password management for home IoT devices [9]

Still, technical mechanisms are essential and consumers prefer to have them to help to deal with their security. Devices that show a clear view of their security level and how to use the features in correct ways could make great improvement to reach this goal. We argue that we need standard metrics that define a common way to evaluate them.

4.5.2 Effects

Defining a limited, known set of metrics and using it to evaluate systems could lead attackers to have a deeper initial knowledge about systems, gaining hints about which components could be more vulnerable. This suggests a question: is secrecy better or worse than disclosure on security issues? Security should not be dependent on secrecy, also because the disclosure of issues let people and companies take actions to improve

defenses. So, in contrast with the intelligence side that is based on secrecy, the cybersecurity world is mainly focused on disclosure (e.g. the MITRE CVE[3] classification) and the same principle applies to CPS.

The standardization of security metrics could allow a unified and reproducible view of security in CPS so that the consumer has a clear understanding about the level of security and can compare it with other systems, taking more precise decisions. In addition to bringing more awareness, defining metrics and making an automated assessment of the systems could also allow to understand what are exactly the vulnerabilities that lead to that security score and which countermeasures against attackers are missing.

As seen before, the set of security metrics can be substantial and, to give time to react quickly under attacks, it's important to show an interface representing them that is quick to read and intuitive.

In this work [39], a novel approach to visualize a set of security metrics is proposed. It allows comparative analysis of their current and previous values and can be used to outline both traditional security parameters (e.g. network flows) and meta-data (e.g. attack impact level), resulting in positive evaluation from the practitioners that use them in the implemented use case. The analyst where allowed to assess the necessity of certain countermeasures before implementing them and recalculating security metrics, allowing to use this technique to compare efficiency of different solutions, supporting the decision on the choice.

Inside companies, through the results obtained from security metrics, organizations' management can locate the technical, operational, or managerial measures which are correctly or incorrectly implemented. These results make it possible to locate the problems and solve them. In this way, security metrics could be a useful lever to release the necessary funds for the information security functions. In addition the use of security metrics makes it possible to check and attest that the activities of the organization are

[3]https://cve.mitre.org

in agreement with the applicable laws and compliance.

Another implication would be on Cybersecurity Insurance (CI) that is a product, still on the exploring stage, that enable businesses and even consumers to mitigate the risk of cyber crime activity. Most common automated scans, as the one cited in 4.4, derive an aggregate score to specifically evaluate the impact in terms of CIA, analyzing only already known vulnerabilities. Instead, being able to assess security of devices by standardized security metrics would give useful and precise information to CI traders, with comparable and consistent knowledge on the situation for more precise cost estimation. This could lead to less expensive CI for consumers and less risks for CI traders.

4.6 Going Forward

In [31] we claim that measuring the security of a system has always been a hot and complex topic that has led to several interesting works on the subject over the years, but there is the opportunity and the strong need for more research, to achieve a multi-faceted result.

Standardization - It is clear that in the recent years the interest about security metrics has increased and with the large amount of metrics and frameworks available, there is the need to create standards, which currently do not exist for CPS as a whole. To reach this goal, it is necessary to understand in depth the type of system that must be analyzed in order to understand the context and the possible threats. In order to achieve standard metrics it is necessary to select the metrics applicable to that context and perform tests to assess how the metrics truly reflect the level of security achieved.

Efficiency - The chosen metrics, in addition to considering the complexity of the context, should yield results in a limited time, with moderate overhead in resource usage. As an ideal, ambitious target, quantitative measurement of specific security properties should be continuously available as input to the decision-making algorithms that drive autonomic subsystems, as well as to orchestrators that plan the (re)configuration of

infrastructures.

For those reasons we argue that a research work should be done to select the best metrics applicable to CPS and to test them in some real applications. Evaluating one metric at a time to find the most accurate ones could permit to establish some standards making the evaluation of security of systems an automatic process, allowing to improve the awareness on their security level and vulnerabilities.

Addressing complex systems - The level of complexity reached by IT systems makes it necessary to use heterogeneous metrics. Even within the purely technical field, different sub-disciplines adopt approaches that are difficult to integrate with each other, and provide results that are not directly comparable. The idea of a taxonomy of security metrics that could help bridging these obstacles is not new (see for example [58], which was to some extent a reply to a more pessimistic take on the subject [14]), yet it has not reached maturity.

Cross-cutting contributions One of the most rewarding, albeit challenging, paths of research has been cited at the beginning of this thesis. Security issues of CPS are mixed with social risks and effects on personal well-being.
A concrete example of a CPS that can be a perfect use case for developing cross-cutting security metrics are vehicular systems, as shown in [26]: just think about the effects of an attack meddling with the sensing, computation, or actuation phases involved in avoiding accidents. Security issues and security-driven choices are intertwined with functional requirements that revolve around safety, privacy, ethical aspects, legal regulations, economic balances, etc. The CPS resilience can be evaluated with a series of vertical metrics combined, as partially introduced in [15]. This topic will be will be further explored in the next chapter.

Chapter 5

Towards interdisciplinary consumer-oriented Security Metrics

The level of complexity reached by current IT systems makes it necessary to use heterogeneous metrics. Complexity brings also consumption related issues making sustainability and efficiency compelling. Let's take the example of decision-making algorithms that drive autonomic subsystems,: they need measurements of specific security properties, continuously available as input. To make this feasible, results should be given in a limited time and with minimum overhead.

Moreover, as we discussed, it's not just a digital problem. The involvement of not only technical factors, in measuring the security of a system, opens new questions and creates new opportunities and needs for more research, to achieve a multi-faceted result. Especially in CPS that are implicated also in social risks and effect on personal well-being, we claim that it's important to go beyond the analysis of technical characteristic of systems to consider interdisciplinary aspects.

Discrimination, constraints on freedoms, privacy loss [16] and any other physical or moral harm to people must be considered security properties to be measured.

The goal of this chapter is to give insights and research trends on such topics regarding

what we consider the focal driving factors of future security metrics to consider: usability, safety, economics, sustainability and fundamental rights.

5.1 Usability

Humans interacting with information systems tend to follow similar behaviours: things that are easier to do are always preferred. That's why *usability* measures how easy it is for a consumer to use a product by both considering the user experience and the security procedures.

Security has a cost which also influences user experience. For example, security measures like Multi Factor Authentication (MFA) or CAPTCHA can hinder the product usability [65].

Another example relies on the choice of a secure password, which usually conflicts with the usability of a product, but choosing a long and complex password is often a better choice from the security point of view. However, a complex password can be easily forgotten by the consumer and for this reason users frequently choose a simple and easily guessable one [16]

Therefore, more security usually leads to less usability and vice versa: what if it were possible to choose and tune the amount of usability and security to reach an optimal configuration for the user?

To achieve that, metrics should consider that high degree of security are not acceptable if they do not ensure a minimum level of usability, that's why there is a need [30] to consider two main aspects of this combined Security and Usability interaction, called "usable security" and "secure usability", to reach an effective security.

These metrics should calculate the level of usability, following basic principles [65] such as representing real user behaviours and observing the interactions by analyzing the

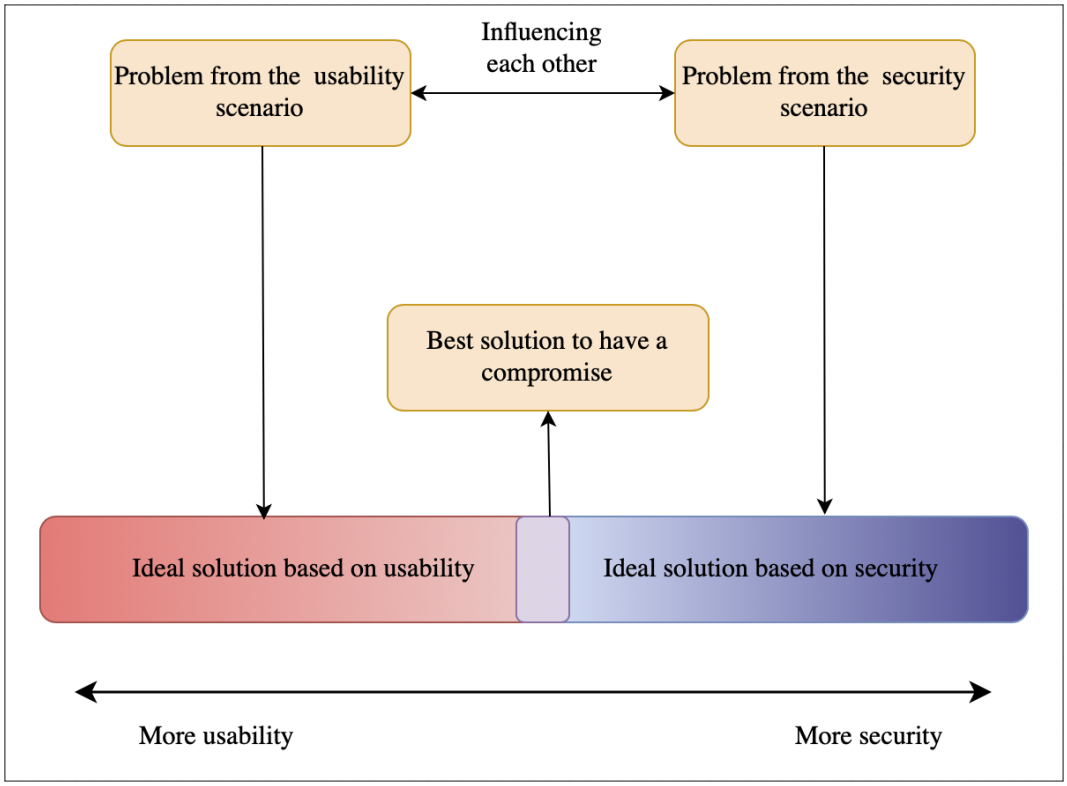

Figure 5.1: Usability and Security trade-off: A common solution based on a compromise.

data obtained. Development processes that try to provides both usability and security already exist [25], but we are trying to define a way to measure it, in particular along the development process.

In [57] authors propose a method to combine and summarize usability metrics in a standardized way, obtaining a unique score that still reaches effectiveness and efficiency. This score could drive security metrics on the evaluation of usability.

5.2 Safety

Safety is not a synonym of Security. While safety aims at protecting life, health and natural environment from any damage that systems may cause, the main goal of security is to protect the confidentiality, integrity and availability of information in the system, threatened by malicious parties [13]. Therefore, secure system do not necessarily need to be safe, and vice versa.
For this reason, it's essential to measure both aspects. Security and Safety must be considered two side of the same story, especially because they can affect each other.

Security algorithms might add crucial delay to the system making it unsafe by slowing the reaction time [71] while some safety procedure could choose to skip some security procedures to grant responsiveness [27].

We argue that there should be a way to estimate the degree of degradation of the overall safety of a system when security mechanisms are introduced in it. This bring to another constraint to consider in security metrics: is safety compromised, and how much, by some security mechanism?

5.3 The social side

Cybersecurity is not only a digital problem, but it also depends on human interactions which are usually referred to as the "weakest link" [70]. CPS use technologies such as cloud computing or IoT devices that increase the attack surface and are very related to the physical world. Therefore, I argue that to give completeness at the way we evaluate security of systems, the real world users interactions must be taken into consideration.

The growth of social media provides cybersecurity actors, both adversaries and targets, with more ways to present themselves in terms of the motivations for their actions and their responses to incidents. This dialogue in turn contributes to the social and cultural context that cybersecurity actors operate within, and which in a case of reciprocal causality is also a determinant of their actions.

LeMay et al. [40] propose a state-based model of a system and the adversary representation which considers adversary attack preferences to mimic the strategy and look ahead on the next most promising move for the attacker, the move estimate costs, payoff and probability of detection.
In this approach, the model can show the difference in time between attacks made by different types of adversary (APT, nation-state, lone hackers and even employees or administrators). An example of index that metrics could use is shown in [18], in which risk-analysis and game theory is used to predict if some targets could be really taken into account in attacks.

Recent cyber-attacks tend to have multi-step approaches where at least one of the phase use social engineering, taking advantage of those "human vulnerabilities" [29]. Social engineering is a term used since the 1842 and it's referred on the idea that one person or group, within a specific domain, enjoys a significant advantage of knowledge over another person or group and "using deception in order to induce a person to divulge private information or esp. unwittingly provide unauthorized access to a computer sys-

tem or network". It is the art of manipulating people through tools such as persuasion, fear, imitation and compassion: it is mainly the non-technical part of a cyber-attack and therefore is the one that typical threat countermeasures, based only on technical details, may skip.

Social engineering can be:

- Human based: involves person-to-person contact such as impersonation, where the attacker pretends to be another person typically with some privilege, for example: an employee, a valid user, a contractor, a third party or even a simple user that needs help calling the help desk for support and instead retrieving the information needed.
- Computer based: involves computer software interactions, such as fake websites, misleading pop-up windows, online scams, baiting, phishing and even spear phishing, that is less common because of it's complexity, but more more accurate and convincing.

Awareness is the key to prevent this kind of attacks, allowing people to protect themselves and avoid to implicitly trust anyone. Thus, focal properties to take into account to elaborate accurate security analysis include also those social and psychological aspects that comprehends:

- social engineering but also the potential behaviour of attacker, including objectives, reactions, but can extends to beliefs and ethical reasons for hacktivists.
- that the attackers can dynamically adapt the strategy based on the situation.
- the economic costs and earnings coupled with the motivations that lead the attacker to pursue a cyberattack.

[0]https://www.oed.com

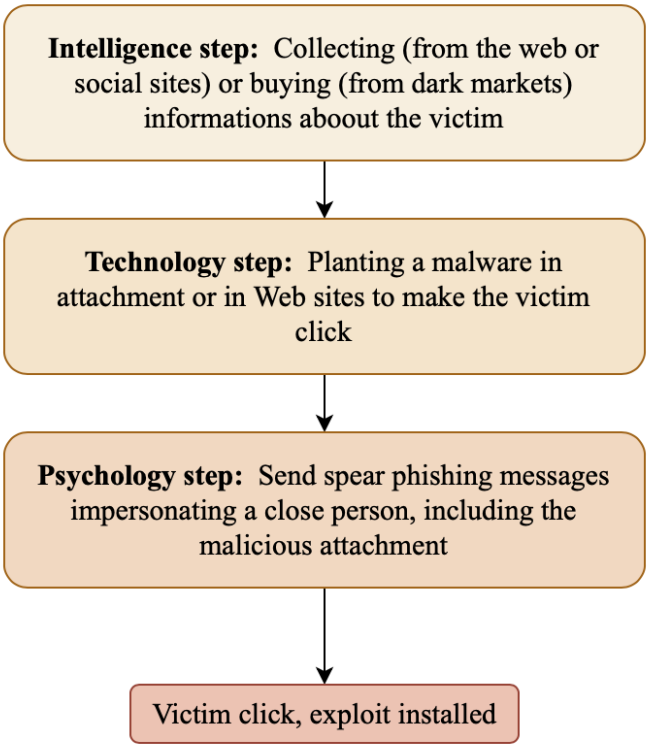

Figure 5.2: Steps that a social engineering attack takes

It is therefore crucial to examining the relationships between an individual user's vulnerability based on his/her cognitive bias or personality traits in order to accurately assess security. Investigating users' personality traits, cognitive biases, and/or disposition and their impact on the users' susceptibility to attacks can be used to design defense mechanisms for mitigating the user's susceptibility to attacks.

5.3.1 Personality as a metric

People often behave in ways that are discordant with how they intend to behave: according to what seen in 4.5.1, people tend to express concern about information security, but few of them actually take action to protect themselves. This may be due to intention

being a cognitive process, whereas behavior is more closely associated with impulsivity in the moment, laziness, distraction or other unconscious processes that require less cognitive effort.

But, can we predict if someone is more likely to be victim of a cyber attack? Can we build a profile of people that are more likely to become victim and use personality traits as a metric? Some recent studies investigates this topic.

The "Big Five" model is one of the most used conceptualizations to understand personality,. It measure five personality traits as shown in table 5.1. In [60] by analyzing current literature, has been demonstrated a connection between personality factors as defined by the Big Five model and cybersecurity attitudes and behavioral practice. Conscientiousness has been most frequently associated with information security behaviors, attitudes, and intentions; however, previous research has documented associations between all Big Five personality factors and cybersecurity practices.

Personality trait	**Description**
Conscientiousness	Impulse control behaviors that help with goal and task completion, such as planning, organizing, and delaying gratification
Openness	The extent to which an individual's mind and experiences are complex and original
Agreeableness	Prosocial attitudes toward others, including traits such as trust and tender-mindedness
Neuroticism	The contrast on emotional stability, includes feelings like anxiety and sadness. Also known as mood instability.
Extraversion	Sociability and an energetic approach to the world

Table 5.1: Description of the Big Five traits

In [60] data were collected from 676 undergraduate participants belonging to ethnically diverse background, with results providing evidence for the association between the personality factors reflected in the Big Five model and self-reported cybersecurity behaviors. Conscientiousness, Agreeableness, and Openness demonstrates to be the most significant factors influencing the results. Using follow-up hierarchical and linear regressions, the study shows that Conscientiousness and Openness explained additional variance over and above other relevant cybersecurity variables, including Perceived Barriers, Response Efficacy, and Security Self-Efficacy.

In [37] was investigated how well self-reported risky cybersecurity behavior could be predicted by a combination of self-reported knowledge about secure passwords and personal characteristics, such as personality traits and general risk-taking in daily life. Results shows that:

- higher levels of **conscientiousness** was related to lower levels of self-reported risky cybersecurity behaviors
- higher levels of **neuroticism** was related to higher levels of self-reported risky cybersecurity behavior
- higher levels of sensation-seeking personality traits and general risk-taking in daily life predict greater use of risky cybersecurity behaviors
- **Extraversion, agreeableness and openness** did observe significant relationships to more or less risky cybersecurity behaviors.

Another study shows that cybersecurity professionals differed from regular IT professionals on Trust, Intellect, Sympathy, Vulnerability, Self- Consciousness, Assertiveness, and Adventurous at the facet level, showing significantly different scores from regular IT professionals in the domains Agreeableness and Openness.

Metrics could also measure the probability of having insider crimes [51], as surveys reveal that 44% of data breaches are the result of insider threats. The fraud triangle, based on motivation, opportunity and rationalization, could be a way to understand

more about what's behind insider crimes.

As we have seen, personality traits are bounded with cybersecurity behavior and, with more research, metrics to assess the tendency to certain attitude could be developed. But, when dealing with people behavior and psycology traits, that represents personal and intimate data, privacy boundary are important. It must be clear that these tools should be used as an indicator to coordinate and enhance crybersecurity training and divulgance inside a company or a group of people and should not be used as a way to discriminate people.

5.4 Sustainability

Information systems are central to the operation of most sectors of industrial society [53] and there is an interplay between security decision and energy consumption [1]. The relation between the two requires complex evaluations, e.g.: can a complex defensive strategy, which is apparently resource demanding, be so effective at thwarting attacks as to minimize consumed resources?

Nowadays, sustainability should be a driving force of any decision and many sectors of society will need to rethink their modes of operation, including cybersecurity.

5.4.1 Smart cities

CPS are at the center of current research about sustainable IT systems, and a example are Smart Cities: they are based on IoT devices and represents the use of information and communication technology to sense, analyze and integrate the key information of core systems in running cities [62]. They could help in the construction of Smart Transportation systems, Smart Tourism and Smart Urban Management.

In the past 5 years, 2 billion people moved in urban areas and we reached almost the 80% of the world's total energy consumption just with cities themselves [10]. Taking China as an example, the household energy consumption in urban areas is always greater than the ones in rural areas, in every region [69].

Smart cities use a management model which mainly focuses on improving urban planning processes to continuously evaluate the resources available. They uses data-driven planning in order to provide to his consumers and citizens, an adequate level of quality of life.
This way, smart cities are placed in a strategic position where a lot of energy is used and the "smart component" makes possible to manage resources in efficient way, avoiding wastes, having a central role in the sustainable process.

[2]https://www.eea.europa.eu/data-and-maps/figures/urban-and-rural-population-in

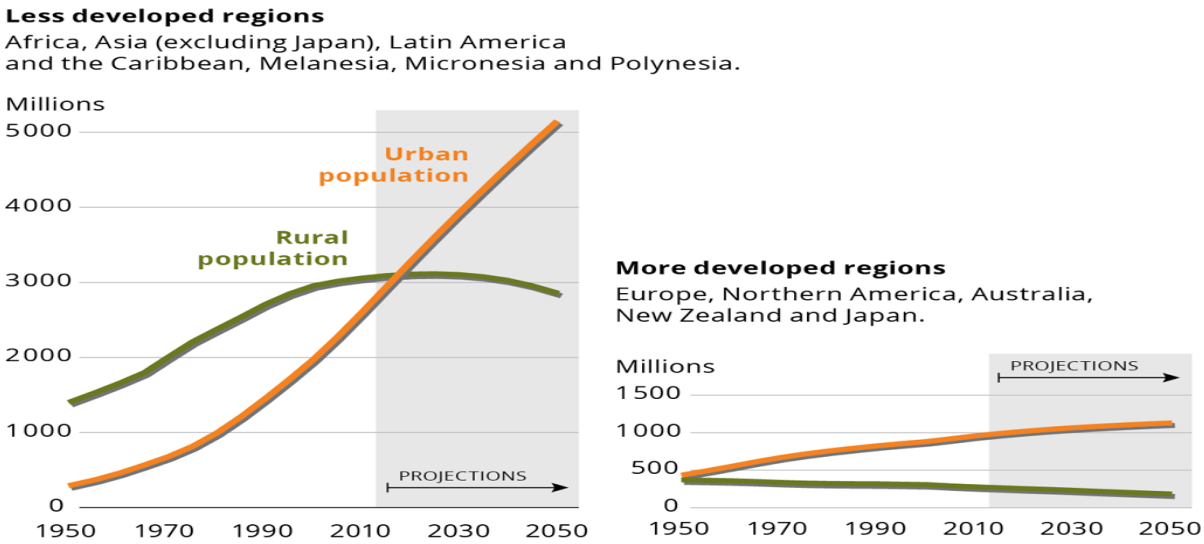

Figure 5.3: Changes of urban and rural population shares from 1950 to 2010 and projected until 2050[2]

Smart cities brought big paybacks to users, who are concerned about the privacy of their data. With all of the data that this technology uses, they are also targeted by criminals and prone to be attacked [33, 46], so countermeasures need to be taken.

Cyberattacks on transportation or smart grid systems could stop cities, and even more[38]. This could have a negative impact on sustainability blocking the smart management of resources and services.

As always, deploying security mechanisms comes with a cost: enforcing a countermeasure could be energy-consuming and for this reason the right compromise between consumption and security should be met. Approaches like Network Intrusion Detection Systems (NIDS) could be very energy-demanding in memory and cpu consumption [23]. Some works were designed with the goal of making them more efficient, modeling their resource consumption, changing configuration and testing how the system behaves, especially for mobile systems.[47].

With security metrics that take into account the performance metrics [27], we can module the overhead of security depending on the impact on consumption, giving the

possibility to manufacturers and consumers to take more sustainable decisions.

5.4.2 A sustainable cybersecurity ecosystem

I argue that cybersecurity is intertwined with sustainability. They influence each other and because of that they should always be considered together everytime.

Malicious online activities are constantly increasing and are among the most dangerous [43]. To stop them, a sustainable cybersecurity ecosystem is crucial in terms of saving and securing organizations from being exploited or suffer data breaches, which often afflicts consumers all over the world [55]. To build those ecosystems, the metrics that we are seeking are essential because they can shows a well evaluated trade-off between the security level and the resource consumption.

Those metrics could evaluate the use of emerging technologies like IoT and blockchain, that could bring new sustainable cybersecurity approaches needed in this ecosystem. Some examples related to the blockchain technology [21] are:

- *Authenticating critical data* that is stored in a decentralized way.
- *Secure data storage*, by keeping cloud data intact and tamper proof with the use of list of hashes that allows secured and verified data extraction and exchange.
- Use of *absolute records of DNS* via encrypted and secured techniques addressing the concerns that led to the slow adoption of DNSSEC. [32]
- *Keyless signature infrastructures*, taking advantage from the timestamp in blockchain, avoid key disclosure, update and revocation.

We have to keep in mind that usually the blockchain introduces intensive computations, especially the ones that reach consensus via the Proof of Work methodology. Different strategies, like Proof of stake and more sustainable alternatives [41] are already being studied to counteract this problem.

Conclusions

Measuring security is essential to understand which countermeasures are the optimal ones to take in devices, system and enterprises. The fundamental question that we want to answer is "How secure is this system?": to formalize an answer, security metrics can be the essential tool that gives precise numbers. They represent a way to make measure of aggregate data overtime, giving the possibility to do realtime assessment on security and rearrange dynamically the countermeasure taken. They can be seen as an effective tool for cybersecurity professionals to calculate the security levels of their systems, products, processes, and readiness to address security issues they are facing.

I analyze the state of the art of security metrics, showing a categorization of them and some real use case scenarios. As said, security metrics can be applied to any kind of context, from the software development to the evaluation on the effectiveness of specific countermeasures. But, changing context lead to change metrics: giving precise security evaluations means to use a specific set of metrics that address completely the security overview of that specific domain.

This problem is analyzed over Cyber-Physical Systems (CPS). Security metrics of any kind are available in literature but only few of them can be applied over CPS: the majority of them is focused on the security analysis of single devices separately and doesn't analyze the effects that happen in deeply interconnected system, such as CPS, that change the situation in the overall security. So, to answer "How secure is this CPS?", there is the need to select and create specific metrics.

There are different ways of generating security metrics, I presented three of them: Classification and selection, Automatic Generation and MLR in 3.5. It's important to minimize the quantity of data to analyze and to keep the number of metrics low, as recommended by other studies, to reach an effective framework. So, to reach the objectives desired, as the ones in the Cybersecurity Act, analyzing the context and creating a model of the system that represents correctly the domain it's essential to reach standardized security metrics.

As security should not be based on secrecy, having an unified view on it would make consumer clearly aware about security of devices, systems, making them comparable security wise between each other. Moreover, the standardization would help automatic assessment, automatic and quick reconfiguration of devices and network component, provide useful control panels, make predictions about certain security configurations supporting preliminary decisions.

That said, it's been explained that cybersecurity isn't related only to technical aspects. It involves different spheres of disciplines, being dependent and having impacts in safety and usability aspects, human factors such as personality, motivation, emotion, sustainability where smart cities were proposed as an example of narrow dependency between technologies and environment.

In order to make real use of security metrics, more research needs to be done on these interdisciplinary topics, so as to go beyond the simple technical analysis of security flaws and analyze the complex interaction with everyday life, creating the foundation for a cybersecurity framework that can answer to the question mentioned before: "How secure is it?".

From a future perspective, creating the right combination of security metrics for CPS can open up new interesting possibilities. As mentioned before, CPS are complex systems, and this affects especially the configuration and reconfiguration overtime that can become tedious. Many recent research focuses on analyzing the scenario where network

devices can self-configure and reconfigure at runtime based on surrounding conditions like consumption, resource violation, change of configuration and more. Those decisions should be made considering security: that's where the metrics find their application, to build a framework that gives the possibility for tuning the parameters and find the most securitywise efficient combination for every device of the system.

Bibliography

[1] From green to sustainability: Information technology and an integrated sustainability framework. *The Journal of Strategic Information Systems*, 20(1):63–79, 2011. The Greening of IT.

[2] Jemal Abawajy. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3):237–248, 2014.

[3] Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky. *Consumer attitudes toward data breach notifications and loss of personal information.* Rand Corporation, 2016.

[4] Nadeem Ahmed, Umme Kulsum, Imran Bin Azad, A S Zaforullah Momtaz, M. Ershadul Haque, and Mohammad Shahriar Rahman. Cybersecurity awareness survey: An analysis from bangladesh perspective. In *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, pages 788–791, 2017.

[5] Rana Khudhair Abbas Ahmed. Security metrics and the risks: an overview. *International Journal of Computer Trends and Technology (IJCTT)*, 41:106–112, 2016.

[6] Andreas Aigner and Abdelmajid Khelil. A benchmark of security metrics in cyber-physical systems. In *2020 IEEE International Conference on Sensing, Communication and Networking (SECON Workshops)*, pages 1–6. IEEE, 2020.

[7] Andreas Aigner and Abdelmajid Khelil. A security qualification matrix to efficiently measure security in cyber-physical systems. In *2020 32nd International Conference on Microelectronics (ICM)*, pages 1–4. IEEE, 2020.

[8] Reem Al-Shiha and Sharifa Alghowinem. *Security Metrics for Ethical Hacking: Proceedings of the 2018 Computing Conference, Volume 2*, pages 1154–1165. 01 2019.

[9] Aniqa Alam, Heather Molyneaux, and Elizabeth Stobert. Authentication management of home iot devices. In *International Conference on Human-Computer Interaction*, pages 3–21. Springer, 2021.

[10] Roberto O. Andrade, Sang Guun Yoo, Luis Tello-Oquendo, and Iván Ortiz-Garcés. Chapter 12 - cybersecurity, sustainability, and resilience capabilities of a smart city. In Anna Visvizi and Raquel Pérez del Hoyo, editors, *Smart Cities and the un SDGs*, pages 181–193. Elsevier, 2021.

[11] Uchenna P Daniel Ani, Hongmei He, and Ashutosh Tiwari. A framework for operational security metrics development for industrial control environment. *Journal of Cyber Security Technology*, 2(3-4):201–237, 2018.

[12] M Azuwa, Rabiah Ahmad, Shahrin Sahib, and Solahuddin Shamsuddin. Technical security metrics model in compliance with iso/iec 27001 standard. *International Journal of Cyber-Security and Digital Forensics*, 1(4):280–288, 2012.

[13] M. Bartnes. Safety vs. security? 2006.

[14] Steven M Bellovin. On the brittleness of software and the infeasibility of security metrics. *IEEE Security & Privacy*, 4(04):96–96, 2006.

[15] Leila Benarous and Saadi Boudjit. Security and privacy evaluation methods and metrics in vehicular networks. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–6. IEEE, 2022.

[16] Davide Berardi, Franco Callegati, Andrea Melis, and Marco Prandini. Password similarity using probabilistic data structures. *Journal of Cybersecurity and Privacy*, 1(1):78–92, 2020.

[17] W Krag Brotby and Gary Hinson. *Pragmatic security metrics: applying metametrics to information security*. CRC Press, 2013.

[18] Ahto Buldas, Peeter Laud, Jaan Priisalu, Märt Saarepera, and Jan Willemson. Rational choice of security measures via multi-parameter attack trees. In Javier Lopez, editor, *Critical Information Infrastructures Security*, pages 235–248, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[19] Elizabeth Chew, Marianne Swanson, Kevin M Stine, Nadya Bartol, Anthony Brown, and Will Robinson. Sp 800-55 rev. 1. performance measurement guide for information security, 2008.

[20] Isabella Corradini. *Building a cybersecurity culture in organizations*, volume 284. Springer, 2020.

[21] Fangfang Dai, Yue Shi, Nan Meng, Liang Wei, and Zhiguo Ye. From bitcoin to cybersecurity: A comparative study of blockchain application and security issues. In *2017 4th International Conference on Systems and Informatics (ICSAI)*, pages 975–979, 2017.

[22] George T Doran et al. There'sa smart way to write management's goals and objectives. *Management review*, 70(11):35–36, 1981.

[23] Holger Dreger, Anja Feldmann, Vern Paxson, and Robin Sommer. Predicting the resource consumption of network intrusion detection systems. In Richard Lippmann, Engin Kirda, and Ari Trachtenberg, editors, *Recent Advances in Intrusion Detection*, pages 135–154, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[24] José Luis Fernández-Alemán, Inmaculada Carrión Señor, Pedro Ángel Oliver Lozoya, and Ambrosio Toval. Security and privacy in electronic health records: A systematic literature review. *Journal of biomedical informatics*, 46(3):541–562, 2013.

[25] Ivan Flechais, Cecilia Mascolo, and Martina Angela Sasse. Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics*, 1(1):12–26, 2007.

[26] Guillermo A Francia III. Vehicle network security metrics. In *Advances in Cybersecurity Management*, pages 55–73. Springer, 2021.

[27] Radek Fujdiak, Petr Mlynek, Petr Blazek, Maros Barabas, and Pavel Mrnustik. Seeking the relation between performance and security in modern systems: Metrics and measures. In *2018 41st International Conference on Telecommunications and Signal Processing (TSP)*, pages 1–5, 2018.

[28] Vahid Garousi, Michael Felderer, and Mika V Mäntylä. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, 106:101–121, 2019.

[29] Ibrahim Ghafir, Vaclav Prenosil, Ahmad Alhejailan, and Mohammad Hammoudeh. Social engineering attack strategies and defence approaches. In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 145–149, 2016.

[30] Oleksandr Gordieiev, Vyacheslav Kharchenko, and Kostiantyn Leontiiev. Usability, security and safety interaction: profile and metrics based analysis. In *International Conference on Dependability and Complex Systems*, pages 238–247. Springer, 2018.

[31] Giacomo Gori, Andrea Melis, Lorenzo Rinieri, Marco Prandini, Amir Al Sadi, and Franco Callegati. Metrics for cyber-physical security: a call to action. In *2022 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–4. IEEE, 2022.

[32] Scarlett Gourley and Hitesh Tewari. Blockchain backed dnssec. In *International Conference on Business Information Systems*, pages 173–184. Springer, 2018.

[33] Bushra Hamid, Nz Jhanjhi, Mamoona Humayun, Azeem Khan, and Ahmed Alsayat. Cyber security issues and challenges for smart cities: A survey. In *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, pages 1–7, 2019.

[34] Allen A Harper. *The impact of consumer security awareness on adopting the internet of things: A correlational study*. PhD thesis, Capella University, 2016.

[35] Jean-Pierre Hauet. Isa99/iec 62443: a solution to cyber-security issues? In *ISA Automation Conference*, 2012.

[36] Jin B Hong, Simon Yusuf Enoch, Dong Seong Kim, Armstrong Nhlabatsi, Noora Fetais, and Khaled M Khan. Dynamic security metrics for measuring the effectiveness of moving target defense techniques. *Computers & Security*, 79:33–52, 2018.

[37] Shelia M Kennison and Eric Chan-Tin. Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology*, 11:546546, 2020.

[38] Oliver Kosut, Liyan Jia, Robert J. Thomas, and Lang Tong. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In *2010 First IEEE International Conference on Smart Grid Communications*, pages 220–225, 2010.

[39] Igor Kotenko and Evgenia Novikova. Visualization of security metrics for cyber situation awareness. In *2014 Ninth International Conference on Availability, Reliability and Security*, pages 506–513. IEEE, 2014.

[40] Elizabeth LeMay, Michael D. Ford, Ken Keefe, William H. Sanders, and Carol Muehrcke. Model-based security metrics using adversary view security evaluation (advise). In *2011 Eighth International Conference on Quantitative Evaluation of SysTems*, pages 191–200, 2011.

[41] Aiya Li, Xianhua Wei, and Zhou He. Robust proof of stake: A new consensus protocol for sustainable blockchain systems. *Sustainability*, 12(7):2824, 2020.

[42] Ángel Longueira-Romerc, Rosa Iglesias, David Gonzalez, and Iñaki Garitano. How to quantify the security level of embedded systems? a taxonomy of security metrics. In *2020 IEEE 18th International Conference on Industrial Informatics (INDIN)*, volume 1, pages 153–158. IEEE, 2020.

[43] Francesca Bosco Mariarosaria Taddeo. We must treat cybersecurity as a public good. here's why. *World Economic Forum*, 2019.

[44] Gastón Márquez, Carla Taramasco, and Hernán Astudillo. Defining security metrics to evaluate electronic health records systems: A case study in chile. In *2020 IEEE In-*

ternational Conference on Software Architecture Companion (ICSA-C), pages 173–180. IEEE, 2020.

[45] Sara N Matheu, Jose L Hernandez-Ramos, and Antonio F Skarmeta. Toward a cybersecurity certification framework for the internet of things. *IEEE Security & Privacy*, 17(3):66–76, 2019.

[46] Andrea Melis, Marco Prandini, Saverio Giallorenzo, and Franco Callegati. Insider threats in emerging mobility-as-a-service scenarios. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[47] Fontanelli Paolo Merlo Alessio, Migliardi Mauro. Measuring and estimating power consumption in android to support energy-based intrusion detection. *Journal of Computer Security*, 23, no5:611–637, 2025.

[48] Patrick Morrison, David Moye, Rahul Pandita, and Laurie Williams. Mapping the field of software life cycle security metrics. *Information and Software Technology*, 102:146–159, 2018.

[49] Carlos Murguia, Iman Shames, Justin Ruths, and Dragan Nešić. Security metrics and synthesis of secure control systems. *Automatica*, 115:108757, 2020.

[50] Jonathan Nield, Joel Scanlan, and Erin Roehrer. Exploring consumer information-security awareness and preparedness of data-breach events. *Library Trends*, 68(4):611–635, 2020.

[51] Keshnee Padayachee. Understanding the relationship between the dark triad of personality traits and neutralization techniques toward cybersecurity behaviour. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 10(4):1–19, 2020.

[52] Marcus Pendleton, Richard Garcia-Lebron, Jin-Hee Cho, and Shouhuai Xu. A survey on systems security metrics. *ACM Computing Surveys (CSUR)*, 49(4):1–35, 2016.

[53] Birgit Penzenstadler, Ankita Raturi, Debra Richardson, and Bill Tomlinson. Safety, security, now sustainability: The nonfunctional requirement for the 21st century. *IEEE Software*, 31(3):40–47, 2014.

[54] Eleni Philippou, Sylvain Frey, and Awais Rashid. Contextualising and aligning security metrics and business objectives: A gqm-based methodology. *Computers & Security*, 88:101634, 2020.

[55] Shahrin Sadik, Mohiuddin Ahmed, Leslie F. Sikos, and A. K. M. Najmul Islam. Toward a sustainable cybersecurity ecosystem. *Computers*, 9(3), 2020.

[56] Dilshani Sarathchandra, Kristin Haltinner, and Nicole Lichtenberg. College students' cybersecurity risk perceptions, awareness, and practices. In *2016 Cybersecurity Symposium (CYBERSEC)*, pages 68–73, 2016.

[57] Jeff Sauro and Erika Kindlund. A method to standardize usability metrics into a single score. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '05, page 401–409, New York, NY, USA, 2005. Association for Computing Machinery.

[58] Reijo M. Savola. Towards a taxonomy for information security metrics. In *Proceedings of the 2007 ACM Workshop on Quality of Protection*, QoP '07, page 28–30, New York, NY, USA, 2007. Association for Computing Machinery.

[59] Reijo M Savola. Quality of security metrics and measurements. *Computers & Security*, 37:78–90, 2013.

[60] Alexander T Shappie, Charlotte A Dawson, and Scott M Debb. Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, 9(4):475, 2020.

[61] Sankalp Singh, James Lyons, and David M Nicol. Fast model-based penetration testing. In *Proceedings of the 2004 Winter Simulation Conference, 2004.*, volume 1. IEEE, 2004.

[62] Kehua Su, Jie Li, and Hongbo Fu. Smart city and the applications. In *2011 International Conference on Electronics, Communications and Control (ICECC)*, pages 1028–1031, 2011.

[63] Khalid Sultan, Abdeslam En-Nouaary, and Abdelwahab Hamou-Lhadj. Catalog of metrics for assessing security risks of software throughout the software development life cycle. In *2008 International Conference on Information Security and Assurance (isa 2008)*, pages 461–465. IEEE, 2008.

[64] Aditya Sundararajan, Arif I Sarwat, and Alexander Pons. A survey on modality characteristics, performance evaluation metrics, and security for traditional and wearable biometric systems. *ACM Computing Surveys (CSUR)*, 52(2):1–36, 2019.

[65] Mary Frances Theofanos and Shari Lawrence Pfleeger. Guest editors' introduction: Shouldn't all security be usable? *IEEE Security & Privacy*, 9(2):12–17, 2011.

[66] Jasper L Tran. Navigating the cybersecurity act of 2015. *Chap. L. Rev.*, 19:483, 2016.

[67] Ju An Wang, Hao Wang, Minzhe Guo, and Min Xia. Security metrics for software systems. In *Proceedings of the 47th Annual Southeast Regional Conference*, pages 1–6, 2009.

[68] Lingyu Wang, Sushil Jajodia, and Anoop Singhal. *Network Security Metrics*. Springer, 2017.

[69] Shubin Wang, Shaolong Sun, Erlong Zhao, and Shouyang Wang. Urban and rural differences with regional assessment of household energy consumption in china. *Energy*, 232:121091, 2021.

[70] Brenda K Wiederhold. The role of psychology in enhancing cybersecurity, 2014.

[71] Michael L Winterrose, Kevin M Carter, Neal Wagner, and William W Streilein. Balancing security and performance for agility in dynamic threat environments. In *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 607–617. IEEE, 2016.

[72] Claes Wohlin. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, pages 1–10, 2014.

[73] Ioannis Zografopoulos, Juan Ospina, Xiaorui Liu, and Charalambos Konstantinou. Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access*, 9:29775–29818, 2021.