SUPREMO AMICUS

INDIA'S FIRST AI INTEGRATED LAW JOURNAL

Peer Reviewed, Refereed and Open access Journal

- Available in 331+ International Libraries
- Indexed at 32 Databases

ISSN NO. 2456-9704
Volume 10 Issue 1
www.supremoamicus.org

DISCLAIMER

The information presented in this article is intended for general informational and educational purposes only. While every effort has been made to ensure that the content is accurate, up-to-date, and reliable at the time of publication, the editorial board and publisher make no representations or warranties of any kind, express or implied, regarding the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

The views and opinions expressed in this article are those of the author and are based on personal research, experience, and interpretation. They do not necessarily reflect the official policy, position, or opinions of any affiliated organization, institution, or entity.

This article is not intended to serve as professional advice of any kind. The editorial board and publisher shall not be held liable for any errors or omissions in the content, nor for any losses, injuries, or damages arising from the use of or reliance on this information.

ABOUT THE JOURNAL

Supremo Amicus is an online, peer-reviewed international journal devoted to the interdisciplinary fields of law and science. In an era marked by rapid technological progress and evolving legal frameworks, the journal seeks to bridge the gap between these two dynamic domains by offering comprehensive and critical insights into their various aspects. The journal places a strong emphasis on contemporary advancements, emerging trends, and the complex challenges faced by both the legal community.

The primary objective of the journal is to encourage and promote original, high-quality research. It is committed to publishing well-researched, analytically sound, and thought-provoking articles that adhere to rigorous academic standards. Each submission undergoes a thorough peer-review process to ensure authenticity, relevance, and scholarly integrity. In doing so, the journal maintains its commitment to excellence and credibility.

In addition to fostering research, the journal aims to make complex ideas accessible and engaging for a diverse readership. It strives to present content that is not only intellectually enriching but also clearly written and reader friendly.

Furthermore, the journal is committed to promoting interdisciplinary collaboration and global engagement. It welcomes diverse perspectives from contributors across different regions and backgrounds, thereby enriching the quality and scope of discussions presented within its pages.

With this vision we proudly present Supremo Amicus to our readers.

-Editorial Team
Supremo Amicus

CYBER SECURITY OF CRITICAL INFRASTRUCTURES: THREAT LANDSCAPES MATURITY MODELS, AND STRATEGIC RESILIENCE

By *Aditya Prakash*
From Amity University, Noida

By *Shailja Khosla*
From Amity University, Noida

Abstract

The growing dependence on digital technologies has shifted the functioning of critical infrastructure systems to achieve more efficiency, automation, and connections in the energy sector, healthcare, transportation sector, and telecommunications sector. Nonetheless, the change has brought about the major cybersecurity challenges as well. Incorporation of Information Technology (IT) with Operational Technology (OT) and Cyber-Physical Systems (CPS) has increased the attack surface such that important services are susceptible to advanced and targeted cyber assaults. Due to this, cybersecurity has become a national and global security issue, rather than a technical one.

This dissertation discusses how cyber threats have evolved and how they affect the critical infrastructure. It also indicates the shift of the isolated instances of cyber-attacks to highly organized attacks by state sponsored actors and cybercriminal groups. It specifically concentrates on the offensive cybersecurity tools, the development of ransomware, and reallife incidents to show that disruption can be universal. The inadequacy of traditional security solutions and the need of more dynamic and proactive security solutions are also discussed in the paper.

The adoption of the existing security frameworks and strategies is one of the areas that this study will be interested in. The paper explores how the Zero Trust Architecture (ZTA) helps in addressing the limitations of the perimeter based security by promoting constant attestations and minimizing lateral flows in the network. It also takes into account the frameworks of the cybersecurity maturity, including the NIST Cybersecurity Framework and the Cybersecurity Capability Maturity Model (C2M2) as the tools of evaluating and improving the preparedness of the organization.

Further, the dissertation includes the governance-related challenges in securitizing the critical infrastructure particularly the loophole between government and ownership by the private sector. It proposes a remedy in the shape of structured Public-Private Partnerships (PPP) that will be supported by the S.A.G.E. system prioritizing safety, responsibility, global cooperation, and engagement with stakeholders.

Other industry-related topics analyzed in the study include the security of Industrial Control Systems (ICS) and smart grids, application of cyber ranges in training and preparedness, and emerging technologies, including post-quantum cryptography. These discussions indicate the need to have a multidisciplinary approach to integrate policy and governance with technical innovation.

The conclusions of this paper would show that the problem of the modern cybersecurity threats does not have a single solution. Instead, it requires a holistic method, including advanced threat detection mechanisms, maturity models, and Zero Trust principles and joint governance paradigms. This is required to create resilient systems that are able to protect critical infrastructures in a more connected and threat prone environment.

Introduction

The Changing Threat Landscape: There are threats to the cybersecurity community, and when they refer to the threat landscape, it is not the physical place that they refer to. They are tracing the ever-shifting map of how digital criminals do business, what they employ and which specific vulnerabilities they would like to take advantage of. That map has gone on a huge tectonic shift now.

Succinctly put: we are relocating to an era, when bank robberies were carried out by brutes, and an era, when they are being carried out in a more systematic, automated fashion, a confidence scheme.

The digital battlefield has experienced the following four big developments over the past few years:

The Death of Hacking (The Identity Crisis).

Some of the biggest threats ten years ago involved the really technical programmers, who were interested in finding the tiniest flaws in a firm firewall so that they could break in. In today's world, attackers barely bother to even make the attempt to break the window digitally. Instead they just walk in the front door with a stolen key.

Thieves hijack your internet identities: your online passwords or the unseen authentication tokens that enable you to stay logged into your applications, with which they log in under the name of a genuine employee. The present day threat is not concentrated on cracking software but it is more focused on exploiting human psychology to steal credentials.

Now, advanced software programmers have created advanced ransomware and sell it to average criminals on a pay-per-use basis- a system known as Ransomware-as-a-Service (RaaS). These criminal gangs operate as legitimate tech startups, such as affiliate profit sharing, human resource offices and even 24/7 customer support call centers to refer victims to the cryptocurrency payment process.

The Pearl Harbor Moment in Cybersecurity The Colonial Pipeline Case.

This concept is identified as a Pearl Harbor moment in cybersecurity and refers to a pivotal moment - an so significant that it compels governments, organizations, and societies to acknowledge the vulnerability that was previously underestimated or overlooked. This is the time of the digital age, when one attack does not happen due to a military action, but due to cyber attacks that demonstrate how much the critical infrastructure relies on a weak and in most cases poorly defensed digital infrastructure.

The Colonial Pipeline attack of 2021 is generally seen as one of the most obvious cases of such an instance. A ransomware group in this attack, the Darkside, was able to hack into the network of the company with a compromised password. The reason why the situation was so alarming was that the account was not secured by a multi-factor authentication feature - a security basic level that would have helped to stop unauthorized access. Although the entry point is quite simple, the effects were dire.

Colonial Pipeline has also been shut down to prevent any leakage and this has stopped almost 5,500 miles of fuel delivery in the eastern part of the United States. Nearly 45 percent of the supply of fuel to the region was disrupted by this disruption. In several days, the effects were manifested in the daily life: fuel shortages began in several states, long queues at gas stations, panic buying exacerbated the crisis. The event also caused the price of fuel to shoot up, and had a more global effect on the economy.

What makes this attack akin to a “Pearl Harbor moment is not only the magnitude of the disruption but also the wakeup call it had. It revealed the potential effects of a failure in one place in a privately-run system that would be felt across the nation. It also established that cyberattacks are not restricted to the virtual realm anymore, as they can have a direct impact on the physical infrastructure and other vital services. Besides, what happened also revealed a bigger structural problem: although critical infrastructure is critical to national security much of it is owned and controlled by private entities. This leaves a loophole whereby there is the sharing of responsibility of security and the fragmentation of control. The Colonial Pipeline attack underscored the fact that the oldfashioned methods of cybersecurity treatment based on considering it as an internal corporate problem are no longer enough.

Essentially, the Colonial Pipeline incident has been a wake-up call. It was a moment when the threats of cyberattacks on critical infrastructure could no longer be disregarded. Similar to the historical Pearl Harbor attack that redefined the approach to military strategy, this cyber incident redefined the way of thinking of countries about security in a digitally connected world.

Offensive Cybersecurity

Regarding the present-day cyber threat, the offensive cybersecurity may be viewed as the collection of strategies, tools, techniques that the attackers use to identify the vulnerabilities, unlawfully access and apply digital systems with a malicious purpose. These methods have over the years, evolved into being a mere opportunistic assaults to systematized and planned assaults. The new-day attackers are typically structured, purposeful and possess high-tech capabilities. This is of particular concern given critical national infrastructure where any small attack can greatly affect the safety of the people, their economic stability and national security.

A mixture of technical mechanisms and strategic planning is one of the most popular features of offensive cybersecurity. Hackers usually do not rely on one technique and implement several techniques to enhance their success probability with minimum chance of being caught. Some of the most popular components used include encryption, network sniffing, web-based attacks and malware deployment. All these have a separate purpose in a greater attack plan.

An example is encryption which is a dual-use technology. Although it is critical in supporting valid communications and ensuring confidentiality of sensitive information, it has been discovered that attackers have found ways of using it as a means of hiding and dominating. Bad programs are mostly coded to evade the classical security programs which use signature detection. Further, the traffic between compromised systems and external command servers is often encrypted and thus it is hard to intercept malicious traffic or detect malicious activity by the defenders. In ransomware encryption is applied more forcefully- files are intentionally encrypted, and they cannot be unlocked by the owner. An encryption is then used as a direct coercion as a victim is pressured into paying a ransom in exchange of decryption keys. Network sniffing is another technique that is important because it entails the capture and analysis of the data packets as they pass through a network. This technique enables the attackers to monitor the system activities, detect the patterns of communication and obtain sensitive usernames, passwords and session identifiers.

Offensive cybersecurity also involves web injection attacks as a very crucial element. These attacks are aimed at web based applications by introducing malicious code into input fields, URLs or even backend queries. Examples that are common are SQL injection and cross-site scripting both of which are based on flawed input validation and insecure coding style. In these methods, attackers are able to compromise databases, steal sensitive user information or have administrative access to web systems. As much of the critical infrastructure services are based on web-based interfaces to monitor and control, these vulnerabilities can be used to gain access to larger and more sophisticated networks.

The effectiveness of each of these techniques is great, but the effectiveness is more about the combination of these techniques in the frame of a structured attack process. This process can be conceptualized as a recipe of success which every stage is based on the next one in order to reach a certain goal. The inaugural phase in this process is reconnaissance where the attackers assemble as much information as they can about their target. This can involve researching on publicly available data, discovery of system designs and scanning of vulnerabilities and even gathering personal information about the employees so that the attack can be socially engineered.

After reconnaissance, attackers proceed to the first access stage, in which they seek to gain access into the system. This may be done in a number of ways

including phishing emails, exploiting of software vulnerabilities or even with stolen credentials acquired during prior activities such as network sniffing. After access has been achieved, it is then time to create persistence, so that the attacker can have a presence in the system long term without being easily spotted and eliminated.

Once gaining access, attackers will often seek to increase their control by lateral movement, moving throughout the network to access more valuable systems and data. At this stage they can increase their privileges and achieve a greater degree of access that can unlock the security restrictions and enable them to perform more meaningful actions. This phase is especially risky in the context of critical infrastructure where networked systems may facilitate attackers to transition between less sensitive domains to the fundamental systems of operation.

The second step usually includes the execution of a malicious code, ransomware or spyware. With ransomware, systems are shut down and data is encrypted, leaving organizations with two options, to pay ransom, or to endure a lengthy downturn. Meanwhile, attackers can also steal resources, by exploiting compromised machines to mine cryptocurrency, initiate other attacks, or fund more run-of-the-mill criminal activities. This does not only enhance profits of the attacker but it also exerts more burden to the infrastructure of the victim.

Lastly, attackers make efforts to leave minimal traces, which lessen chances of being detected and extend their stay in the system. This may involve deleting logs, disguising malicious activity as a legitimate system operation, or communicating encryptively so as to be undetected.

The attack would be identified later and a significant amount of damage would be incurred. In conclusion, the field of offensive cybersecurity has been developing into a highly structured and multi-layered one which is also incredibly difficult to existing security systems. These attacks are difficult to both prevent and detect since they are coupled with advanced tools, strategic execution and a process of constant adaptation. When it comes to the critical national infrastructure, the stakes are very high, as the successful attacks can impose a burden on the important services and affect millions of lives. Understanding what and how an offensive cybersecurity is capable of, should be a requisite step toward developing working defenses and resiliency over the long-term in a threat environment that is increasingly becoming more complex.

• Ransomware Evolution

Ransomware is quite a recent form of cyberattack, and one of the most disruptive forms over the past few years, particularly of critical infrastructure. What began as quite simple malicious programs, has since evolved into quite an organized and profitable cybercrime paradigm. The modern ransomware attacks are more focused, and more frequent because they are typically based on inflicting the most significant effect and profit on the operations. In order to develop an appropriate defense system, it is essential to understand how the ransomware has developed, and what different types of ransomware can take.

Fundamentally, ransomware is a form of malware that deprives users of their systems or data and requests them to pay money to get it back. But not every ransomware works in this manner. In general, it can be divided into two major types: crypto-ransomware and locker-ransomware, both having their unique features and consequences.

The more common and harmful one is crypto-ransomware. It has the effect of encrypting files in the system of a victim such that the files are not accessible without a decryption key. After the encryption process has been finished, the attacker will request a ransom-typically in cryptocurrency- to be paid in order to regain access. The most threatening aspect of crypto ransomware is that it can propagate silently across the networks with the activation taking place. A lot of vital information can be encrypted before the attack is

noticed. This can bring the functioning of the sector, like in health care or energy sector, to a stop, leaving organizations with few options to make trying to make decisions under pressure.

Conversely, files are not usually encrypted by locker-ransomware. Rather, it limits the access to the system itself by locking the user interface or blocking the normal operations. The victims can experience failure to log in, operate applications, and communicate with their devices. Although the underlying data might be unharmed, failure to access systems can still be very disruptive particularly in a setting where constant running is a requirement. Lockerransomware can be easier to recover than crypto-ransomware, but it is no less threatening since it has an instantaneous impact on usability.

Ransomware detection and prevention remains a big challenge despite the advancement of cybersecurity. The traditional defense measures such as misuse based detection systems are founded on the identification of known patterns/signatures of malicious software. Though they are efficient with the previously recognized threats, the systems can barely identify new or modified ransomware threats. Attackers usually tweak their code to avoid detection and signature-based techniques are not as reliable.

Even anomaly-based detection systems which are founded on the detection of abnormal behavior within a network have their limitations. They can detect abnormal activity, with a big false positive rate. This can overwhelm security teams and it might be difficult to detect whether an anomaly is valid or not a threat. False alarms may postpone the necessary steps to be implemented in a fast-paced setting, i.e., the ransomware might be running long before anyone can take action.

Under these limitations more versatile and intelligent detection methods are needed. One of the promising solutions is streaming analytics that is founded on the applications of machine learning. Machine learning models can handle high volumes of data in real time as opposed to the traditional systems that can only be used to determine the existence of certain patterns that may be a sign of malicious activity. Only by continually learning new information will these systems be able to react to new threats, including some that the system has never encountered (zero-day) versions of ransomware.

This is also accompanied with streaming analytics that enables checking of system behavior in real time. It does not process the information in batches, rather processes the information immediately it is generated which allows quicker detection and response. An example is when there is an unexpected change in the access patterns of files, indicating the abnormal encryption activity or the system is acting abnormally, this can be identified immediately. Such live knowledge plays a crucial role in preventing the proliferation of ransomware in networks and causing a large-scale damage.

In conclusion, ransomware is a sophisticated and multi-faceted threat, which will continue to compromise the existing security mechanisms. The difference between crypto-ransomware and locker-ransomware assists to demonstrate the numerous opportunities how attackers can impact the systems, yet both kinds underline more powerful and adaptive defense mechanisms should be taken. Traditional detection techniques are still helpful, but can no longer exist on their own. The introduction of machine learning and real-time analytics is a significant advancement towards ransomware attacks detection and prevention, particularly the emergence of novel types of attacks with which they are not familiar. Such advanced methods will be required in protecting critical systems and operational resilience with cyber threats being constantly evolving.

Cybersecurity Maturity and Evaluation frameworks.

The Reason behind the evaluation.

With the evolution of cyber threats and their increasingly sophisticated and unpredictable nature, the approach to security based on ad hoc and reaction is no longer an option. Rather, there is an increased

necessity to have systematic methods that enable them to have a clue on the effectiveness of their cybersecurity practices. In this place, cybersecurity maturity and assessment schemes come in handy.

Simply, cybersecurity maturity can be defined as the level at which an organization is ready to prevent, detect, and react to cyber threats. Not every organization works at the same level- some organizations will have the simplest protection in place whereas others may be adhering to well-established security processes which are undergoing constant enhancement. In the absence of a definite evaluation technique, it is hard to understand the position of an organization and what to do to improve it.

Capability Maturity Models (CMM) can serve as the answer to this issue. These models provide a systematic means to evaluate cybersecurity practices through the decomposition of the practices in various levels of maturity. Each tier is used to denote a development stage, as at the start, the practices are informal or inconsistent, and the development process will focus on streamlining the systems to become optimized and continually improving. This is a step-by step format which allows organizations to assess their present state and strategize on how to improve in the future.

The major benefits of maturity models usage are that they enable organizations to compare their security position with the best practices. Organizations can now compare their processes with best practices and detect loopholes in their defenses instead of basing it on the assumption or isolated measures. This comparison aids in prioritization on areas that there is an urgent need to be addressed like incident response planning, access control or risk management.

The other key advantage is that maturity models give rise to a transition between a reactive and proactive model. Instead of reacting to cyber incidents once they have taken place, organizations are advised to develop robust, repeatable procedures that lower the chances of attacks, in the initial stages. In the long run, this results in greater predictable and trustworthy security results. Such assessment is more needed in the case of critical infrastructure. These systems are likely to be in complicated environments with failure that can have extensive effects. With the help of maturity models, operators will also be in a position to ensure that their cybersecurity practices are effective not only in the level of risk they face.

Further, maturity structures aid in the promotion of decision making at both technical and management levels. They provide first hand information that can guide investments in cybersecurity to make sure that organisations invest in areas that are most needed. It is especially applicable in such environments that are budget strained and time and again priority matters.

In conclusion, CMMs mark a significant step in the right direction, to build more resilient and robust cybersecurity infrastructures. The models can help organizations to leave the guesswork and a more professional approach towards security through offering a well-defined framework on how the assessment and enhancement can be achieved. Such frameworks are necessary not only a tool in an era in which cyber risks continue to evolve in form but a necessity to be guaranteed protection and security over time.

- **Cybersecurity Capability Maturity Model (C2M2).**

Cybersecurity Capability Maturity Model (C2M2) is designed to help organizations, particularly those in the sectors that are vital to the economy like energy to analyze and optimize their cybersecurity operations in a methodical way. It is not intended to be technical, but practical so that organizations can be able to know their current security posture, and to continually add to it as time goes by.

C2M2 is built upon ten key domains that represent key areas of cybersecurity. These include risk management, asset/system management, identity and access control and threat and vulnerability

management. The model ensures that cybersecurity is not perceived as a singlepurpose since with large covers of areas, practices are intertwined and must be collaborative.

The main feature of C2M2 is their Maturity Indicator Levels (MILs) which are in the range between MIL 0 and MIL 3. The levels help organizations in being aware of the degree of maturity in their practices in cybersecurity. The activities could be uncharacterized or incomplete at MIL 0. As organizations evolve to MIL 1, they begin to establish themselves to simple practices that they engage in, but may not be steady yet. These practices are formalized, written and reproducible at MIL 2. Finally, in MIL 3, not only is there the developed process of cybersecurity but it is also controlled and constantly improved.

This development is gradual and this fact allows C2M2 to be particularly useful to organizations, which may lack advanced cybersecurity systems. It very slowly promotes incremental improvement over short term perfection, which helps organizations to build higher defenses over time.

Another consideration is that C2M2 is a practical implementation-oriented. It does not just indicate what is required to be done but also helps organizations to know whether the measures that are implemented are effective or not. The gaps are easier to identify, prioritization of actions and allocation of resources is done more efficiently.

C2M2 has significance to enhance the resilience within the critical infrastructure. It helps organizations to ensure that the practices they are engaging in in cybersecurity are in line with the level of risk they are subjected to by providing a clear guideline on how it can be assessed and enhanced. These well-planned strategies are essential towards maintaining stable and secure operations as cyber threats continue to evolve.NIST Cybersecurity Framework: NIST Cybersecurity Framework (CSF), on the other hand. The NIST Cybersecurity Framework:

Among the most widespread guidelines to organize and improve the cybersecurity, especially the critical infrastructure sphere, NIST Cybersecurity Framework (CSF) is one of the most popular. Since it was developed to provide an intuitive and adaptable approach, it can help organizations gain an understanding of their risks and have a strong security practice without necessarily applying an inflexible one-size-fits-all model.

The 5 basic functions of the framework are: Identify, Protect, Detect, Respond and Recover. These operations are the key milestones towards cybersecurity risk management. Identify is hinged on the knowledge of the assets, systems and the potential risk. Protect involves putting security provisions in place to prevent accidents such as data protection and control. Detect is to make sure that the organizations can quickly become aware that something unusual or hazardous is taking place. Respond talks about what is to be done once a threat has been identified and Recover talks about having a system recovery and proceeding with the activities after an incident.

All these functions are a cyclic process, rather than a one time process. Organizations should undergo these stages periodically and it makes them more skilled in handling threats as time goes by.

• **Industrial Control Systems (ICS) and Smart Grids security.**

Information Technology vs. Operations Technology Security.

The basic distinction between Information Technology (IT) and Operational Technology (OT) is one of the most significant troubles in securing the Industrial Control Systems (ICS). They were initially oriented to very different priorities, although now they are becoming more and more closely related to each other.

IT systems get primarily involved with data protection. The main concern they have is on confidentiality, integrity and availability of information. When it comes to such a setting, the temporary unavailability

can be tolerated in case it will help to eliminate a security breach. An example is that a system can be shut down or patched without any real-life implications.

OT systems on the other hand are in charge of physical processes like generation of electricity, water treatment and manufacturing process. In this case, reliability and safety are the key factors. Even a minor failure can have severe repercussions, such as equipment destruction, service failure, or human life endangered. Due to this reason, most of the OT systems are configured to be up at all times and cannot be updated easily and put offline.

The difference poses a problem in the implementation of cybersecurity measures. Techniques that can effectively be used in IT systems, like regular updates or restricted access, are not necessarily feasible in OT systems. Therefore, the balance between the need to ensure operational stability and enhance security is delicate in securing ICS.

This section will examine the process of identifying the exposed ICS Assets.
As industrial systems continue to become more connected, it is becoming common to have many ICS components that are accessible via the internet, often unintentionally. Such unprotected systems may frequently be identified via Open-Source Intelligence (OSINT) solutions like Shodan that scan the internet to identify devices and services that are connected.

One of the most serious issues is that not all such exposed interfaces have control panels or dashboards that can be directly accessed to control some vital operations. Determining and ensuring these systems is thus an important measure in mitigating risk.

The most recent methods have been investigating how deep learning methods can be used, specifically Convolutional Neural Networks (CNNs), to identify and classify exposed ICS assets. Inception-ResNet-V2 and MobileNet-V1 models are capable of analyzing pictures or screenshots of system interfaces and deciding whether they should be considered as a part of industrial control or not.
The advantage of this approach is that it scales up the vulnerability system identification process, which is automated. Rather than manually screening out thousands of images, machine learning models can rapidly screen and categorize images, assisting security teams to target the most pressing exposures. Using OSINT data and smart analysis, entities will have a better understanding of the possible threat and respond in time to ensure their systems are secure.

ICS Security Policies assessment

The evaluation of the effectiveness of cybersecurity policies in the industrial setting is not an easy task. In comparison to the traditional IT systems, ICS are used in the atmosphere of uncertainty, and risks may change depending on the operational factors, environmental conditions, as well as on the system configurations.

Interval-Valued Complex Intuitionistic Fuzzy Relations, are advanced mathematical techniques that can be employed to tackle this complexity. The terms might be technical, but the concept is rather simple: the methods enable making decisions in circumstances where the information is not complete or is uncertain.

With this policy in place, organizations would be able to try implementing things such as the Default-Deny policy where no access is given unless permitted and the Proactive Protection where emphasis is placed on preventing and stopping threats. Fuzzy logic would also allow for a more forgiving policy when making security decisions. These can be made to sound like yes or no questions but can be better analyzed by looking at the different levels of risk and effectiveness. This could be greatly beneficial in the industrial sector because there has to be balance between the high-level of security that is required and what is needed for operations to run. By utilizing these evaluation methods, organizations will be able to know what it can do to better its security stature when it undertakes it. Additionally, they will know how effective their policies are when placed under different circumstances.

• Governance, Regulation and Public- Private Partnerships (PPs).

The Capability–Responsibility Gap

There exists a capability–responsibility gap.

One of the biggest challenges associated with securing critical infrastructure is who is actually responsible for doing it. Governments have always had the responsibility of providing security for their countries. By extension, they should be securing important infrastructure such as electrical, transportation, hospitals and communication systems. However, it is actually privately owned.

Statistics shows that majority of these systems are– dependant on who you ask, all of them– owned and operated by private companies.

This creates a dynamic where there is inconsistency in structure. Governments are criticized for not providing stability within a country yet they do not have complete say on the majority of systems they should be protecting. On the other hand, there are private companies who own and operate the majority of these systems but may not have the same capability or desire to protect these critical systems from large scale threats.

What you end up getting is a gap between capability and responsibility. You have government who have the regulatory responsibility and ability to provide nationwide coverage but lack the knowledge on the infrastructure and how it operates, which is managed by private companies. Neither party can efficiently protect critical infrastructure from cyber threats on their own. This could also lead to information being siloed and slow response to threats if there is no coordination.

There needs to be a middle ground where there is give and take between individual efforts; the governments and private companies should not be able to operate independently when protecting critical infrastructure.

Government instructions: NIS2 Case.

Governments and regulatory bodies have had to take more stringent measures to better handle the growing cybersecurity threat landscape. One of the biggest initiatives that have been introduced is the NIS2 Directive by the European Union. NIS stands for network and information security. It was created to better handle cyber risks faced by member countries. NIS2 is an extension of the original NIS directive with some improvements. For instance, it not only covers technology companies and organizations that provide essential digital services but has expanded its coverage to include energy, transportation, healthcare sector, banks, and digital service providers. Recognizing that an incident in any of these sectors could have catastrophic consequences to everyday life.

One of the biggest changes is incident reporting. "Essential" organizations will be required to report major cyber incident within 24 hours of realizing the attack. The idea is that, by having this rule, it allows for quick awareness at the national level and Europan level.

Another key change is holding companies liable. Specifically, tier 1 organizations will be held accountable by ensuring that the senior management is making an effort in having proper cybersecurity measures. It shifts cybersecurity efforts from being a technical problem to an organizational governance problem. Non-compliance to some of these requirements could land the companies in serious trouble; heavy fines and loss of reputation.

All in all, this directive is a step in the right direction. The fact that governments are holding companies liable for poor cybersecurity posture is a huge leap towards having better and more regulated cybersecurity standards.

S.A.G.E. model of Public-Private Partnerships.

Regulations can only do so much. The most effective cybersecurity measures always involve some sort of government and non-governmental collaboration. To achieve this, there needs to be more structure when it

comes to public-private cooperation. The S.A.G.E. Tm framework highlights one of many models which is built on four pillars: Safety and Security, Accountability and Ethics, Global Governance, and Engagement and Privacy.

Safety and Security

The main focus of this section is the need to have mutual threat consciousness and act accordingly. Government and private organizations should have a working threat intelligence architecture where information on potential threats are distributed in real-time. Additionally, running cross sector cyber drills can allow organizations to test how they would handle large scale cyber incidents and allow them to work together.

Accountability and Ethics

Trust is important in any relationship. Some organizations will be hesitant to share information whether it be due to legal implications or simply not wanting the world to know they were hacked. To remedy this, legal protection should be established so organizations will not be held liable for sharing cyber threat intelligence with one another. Ethical guidelines should also be put in place to provide oversight on how shared information is being used.

Global Governance

Cybersecurity does not stop at borders. International threat actors are very common and most cyber laws are not compatible with each other. This pillar focuses on the need to have international cooperation and maybe a universal set of cybersecurity regulations. By better aligning various legal and regulatory regimes, it'll allow countries to have a more concerted effort when handling international cyber threats and prevent loopholes during implementation. Engagement and Privacy

Last but not least, the impacts to society should be addressed when handling cybersecurity. This would mean involving stakeholders in the decision making process. This includes anyone from companies, security experts, policy makers and your everyday citizens. Privacy also should be take into consideration when developing systems. Privacy should be designed into the system from the beginning and should not endanger the security of the system just to cater to privacy.

• Future Work

While this thesis provides an extensive explanation of current methodologies and challenges, there are several other areas that can be researched in the future. As the cybersecurity landscape evolves, new technologies and frameworks should be developed to meet new threats. One of the best areas would be creating an automated Zero Trust solution. Although ZTA is gaining a lot of traction right now, most solutions are still configured manually and operated by humans. Research can be done to develop systems that utilize AI to dynamically apply access controls, recognize anomalies and respond to threats automatically. Automated systems would lessen the burden of security teams and improve both efficiency and accuracy. Another field of research would be the integration of artificial intelligence in cybersecurity. AI has already shown great promise in improving threat detection but needs to be improved on. Improving its explainability, reducing false positives, and ensuring reliability in high consequence environments are some of the areas that should be looked into. Research on blending machine learning with human expertise can yield faster and more accurate security solutions.

Another issue that should be addressed is the fragmentation of cybersecurity regulation worldwide. Cybersecurity guidelines and standards are specified by different governments and organizations around the world. This poses a problem to multinational companies since their operations may span multiple jurisdictions. Future efforts should be put towards harmonizing these regulations, allowing for interoperability and having standard guidelines for information sharing and incident response. Cybersecurity should be a collective goal and properly integrated regulations can make world-wide cybersecurity much stronger.

Post quantum security also needs to be focused on. As mentioned earlier, current encryption can be broken by quantum computers if they become powerful enough. Researching on latticebased cryptography, PUFs and other quantum resistant algorithms should be the main focus when dealing with future security.

Improvements can also be made to cyber range technology. Cyber ranges today provide great training opportunities but there is always room for improvement. Integrating technologies such as digital twins, real time data feeds and better simulation models can create the best training environment possible. Professionals can be better equipped on how to handle complex cyber attacks if they are provided a realistic training environment.

Finally, cybersecurity should put more emphasis on human factors. Unlike system vulnerabilities, humans are often the weakest link and are subject to manipulation. Social engineering, phishing, and other tactics that exploit user behavior are used in the most successful breaches. Having research focused on user awareness, behavior analysis and organizational culture can help supplement your technical defences.

*****

• References

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. U.S. Department of Commerce.

- U.S. Department of Energy. (2014). *Cybersecurity Capability Maturity Model (C2M2)*.
- European Union. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*.
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
- Stallings, W. (2018). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.
- Andress, J. (2019). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Syngress.
- Green, M., & Smith, M. (2016). *The Cryptopals Crypto Challenges*. Cryptography Research.
- Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things Journal*, 4(6), 1802–1831.
- Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A Survey of Cyber Security Management in Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, 9, 52–80.
- Roman, R., Zhou, J., & Lopez, J. (2013). On the Features and Challenges of Security and Privacy in Distributed Internet of Things. *Computer Networks*, 57(10), 2266–2279.
- Shodan. (2023). *Search Engine for Internet-Connected Devices*. Retrieved from https://www.shodan.io
- MITRE. (2020). *ATT&CK Framework for Enterprise Security*