Problem Chosen F	2025 MCM/ICM Summary Sheet	Team Control Number 2500778

The world is becoming increasingly reliant on advanced technologies, transforming both industries and societies. Blockchain technology and cryptocurrencies have revolutionized financial systems, offering decentralized, secure, and transparent alternatives to traditional currencies. Advancements in large language models (LLMs) and artificial intelligence (AI) are reshaping fields such as healthcare, education, and cybersecurity, driving efficiency and innovation at unprecedented rates. Emerging technologies like quantum computing further promise to redefine problem-solving capabilities across disciplines, presenting both opportunities and risks as global reliance on digital systems grows [13]. As the limit for what technology can do is constantly changing it is paramount that cybersecurity is constantly re-examined to meet the necessary requirement to protect data and the integrity of users.

Cybercrime poses threats to economies, governments, and individuals, highlighting the need for effective national cybersecurity policies. As technological advancements grow so does the attack surface that can be exploited by adversaries to scam individuals out of hundreds to thousands of dollars or cripple a country's entire infrastructure. The proposed solution intends to develop a theory for effective cybersecurity policies by analyzing global data from the Global Cybersecurity Index (GCI), governance studies, and the National Cybersecurity Guide (NCS Guide). It highlights five pillars—legal frameworks, technical measures, organizational strategies, capacity building, and international cooperation—as essential to mitigating risks. For example, nations with strong Computer Incident Response Teams (CIRTs) and comprehensive education initiatives have shown resilience against ransomware and phishing attacks, while public-private partnerships and international agreements bolster defenses.

Data-driven analysis reveals clear patterns: high-income countries face frequent attacks due to their digital assets, while emerging economies experience increased threats as their infrastructures grow and serve as a “training ground” for beginner hackers. Demographic factors like internet penetration, education, and GDP also play a significant role in cyber resilience. To address gaps, a multi-level approach to national cybersecurity policies continues to build off the baseline of cybersecurity standards and also allows for continual growth while meeting security standards and safeguarding critical infrastructure. By adopting these measures in policies, nations can strengthen their cybersecurity frameworks and protect their digital future, continuing to evolve to meet the ever-changing demands of technology.

Problem Chosen F	2025 MCM/ICM Table of Contents	Team Control Number 2500778

Table of Contents

Problem Chosen F	2025 MCM/ICM Table of Contents	Team Control Number 2500778

Problem Chosen F	2025 MCM/ICM Solution	Team Control Number 2500778

Developing a Strong Theory for National Cybersecurity Policies and Data-Driven Analysis

Introduction

Cybercrime poses significant threats to global security, economies, and individuals. An effective national cybersecurity policy is a necessary and critical key to mitigate these risks. This solution develops a theory for effective national cybersecurity policies by analyzing data from the Global Cybersecurity Index (GCI) [1], systematic reviews of cyber risk [3], governance studies [2], and good practices outlined by the National Cybersecurity Guide (NCS Guide) [4] and other sources. By examining this data, the solution identifies patterns of both effective and ineffective policies and highlights correlations between cybercrime distribution and demographic factors.

Theory of Effective National Cybersecurity Policies

A strong national cybersecurity policy is grounded in five foundational pillars:

Legal Framework

Clear laws and regulations addressing cybercrime, data protection, and data breach notification are key components of an effective cybersecurity policy. According to the GCI 2024, 177 countries have implemented at least one regulation related to personal data protection or breach notifications, with 151 of those countries enforcing data protection measures [1]. Nations that lack these legal frameworks often face higher costs from data breaches and reduced public trust in digital services [3].

The NCS Guide shows the importance of establishing the proper procedures to ensure transparency in enforcing cybersecurity laws and recommends engaging public-private partnerships to strengthen trust in these frameworks [4]. From a global standpoint the legality aspect of cybersecurity is where countries and regions have a well-developed and efficient plan. Ensuring that these policies align with a nation's technology and fiscal capabilities is necessary to ensure optimal effectiveness of the policies.

Technical Measures

Effective technical measures, such as the establishment of Computer Incident Response Teams (CIRTs) and the adoption of cybersecurity standards, show a direct correlation of a

country's cyber resilience. As of 2024, 139 countries have active CIRTs, and 83 are engaged in regional CIRT associations, showing a strong trend towards technical collaboration [1]. This reduces response times and mitigates the effects of large-scale cyberattacks [3].

According to the NCS Guide, regular cybersecurity drills and incident response exercises, like those implemented in countries with advanced CIRTs, significantly improve response capabilities [4]. Maintaining vigilance in up-to-date training and information sessions ensures an all-around knowledge base of the fundamentals and current events occurring in cybersecurity.

Organizational Strategies

National cybersecurity strategies are a critical component of governance. The GCI reports that 132 countries have developed comprehensive national strategies, with 94 incorporating child online protection initiatives [1]. This demonstrates the importance of defined roles, action plans, and regular audits to evaluate progress [3].

Organizational strategies must also include metrics to measure success, as outlined in the NCS Guide. Countries like Finland and Estonia have implemented robust auditing systems that include specific cybersecurity key performance indicators (KPIs) [4].

Capacity Building

Public awareness campaigns and educational initiatives are essential for reducing human-induced errors in cybersecurity. For instance, 152 countries conduct awareness initiatives, while 153 have integrated cybersecurity into their national curricula at various levels of education [1]. This has a direct impact on reducing incidents caused by phishing and ransomware attacks, which often rely on exploiting user mistakes [3].

The NCS Guide stresses that capacity-building efforts should also target underserved communities and SMEs, as these groups often lack access to robust cybersecurity resources [4].

International Cooperation

Collaborative agreements strengthen cybersecurity frameworks. The GCI highlights that 166 countries participate in international cybersecurity agreements, and 122 report interagency collaboration, indicating the growing importance of shared responsibilities and resources [1]. Countries actively engaged in international agreements tend to have better incident response times and access to shared intelligence [3].

Problem Chosen F	2025 MCM/ICM Solution	Team Control Number 2500778

Best practices from the NCS Guide include establishing cross-border incident reporting standards and facilitating joint cyber operations during large-scale cyberattacks [4].

Data-Driven Analysis

Global Cybercrime Distribution

Targets of Cybercrime

High-income nations, such as the United States and countries in the European Union, are frequent targets due to valuable digital assets and interconnected infrastructures, as well as the intel and power these countries hold on the global scale In 2020 alone, cybercrime cost the global economy nearly $1 trillion USD, with most losses being concentrated in developed economies [3]. This number has only continued to increase with an almost staggering 10x increase of $9.5 trillion USD in 2024 [13].

Emerging economies are increasingly targeted as their digital infrastructures expand. For example, regions in Asia and Africa are experiencing significant increases in ransomware and phishing attacks [1]. While these areas hold less value for attackers the continuance of cyber-attacks threatens to hinder the advancements of these regions. Implementing effective policies is one way to ensure the continuance of technological growth for developing nations.

Cybercrime Success Rates

Nations with limited technical and organizational measures experience higher success rates for cyberattacks. The GCI identifies that countries lacking active CIRTs or national action plans face significantly higher incidents of data breaches [1]. However, regions with advanced CIRTs report faster recovery and containment of incidents [3].

Reporting and Prosecution

High-performing countries on the GCI, such as Singapore and the United States, exhibit robust reporting and prosecution mechanisms. Conversely, underreporting remains a challenge in lower-income regions, hindering accurate analysis and response [1][3].

Problem Chosen F	2025 MCM/ICM Solution	Team Control Number 2500778

Patterns in Cybersecurity Policies

Analyzing national strategies reveals

Legal Measures

The presence of comprehensive legal frameworks correlates with reduced data breach incidents. For example, the European Union's General Data Protection Regulation (GDPR) has significantly reduced breach-related costs. Since its implementation, GDPR fines have exceeded EUR 4.5 billion, underscoring its enforcement power and serving as a deterrent against lax cybersecurity practices [3].

Technical Measures

Investment in CIRTs and adherence to cybersecurity standards improves resilience. Data shows that 83 countries engaged in regional CIRT collaborations report fewer vulnerabilities, demonstrating the effectiveness of shared expertise [1]. Countries like Estonia have set an example by integrating CIRT capabilities with a broader e-governance strategy [4].

Organizational Measures

Countries conducting regular cybersecurity audits and protecting critical infrastructure see fewer disruptions. For instance, 104 nations have critical infrastructure regulations, reducing risks in energy, healthcare, and finance sectors [1][3]. Audits allow governments to pinpoint vulnerabilities and prioritize mitigation efforts [4].

Correlation with Demographics

Internet Penetration

High levels of internet access are associated with an increase in cybercrime incidents but also support resilience through greater public awareness and reporting. For instance, countries with over 75% internet penetration report more phishing attempts, but success rates are lower due to greater public familiarity with cyber threats [1][3]. Additionally, countries with high internet penetration invest in more robust cybersecurity measures, contributing to better defense strategies against cyber-attacks [5].

Education Levels

Countries that integrate cybersecurity education at both primary and tertiary levels experience fewer incidents related to human error. According to the Global Cybersecurity Index (GCI), 153 nations have included cybersecurity in their national curricula,

significantly reducing vulnerabilities [1]. Finland's strong emphasis on cybersecurity education, for example, has contributed to its high GCI ranking [4]. Similarly, nationwide cybersecurity awareness initiatives have demonstrated their importance in reducing human error and bolstering overall defense mechanisms [8].

GDP and Wealth

Richer nations are more likely to invest in advanced cybersecurity infrastructure. For example, the average cost of a data breach in high-income countries is $4.45 million, while low-income regions face more significant societal impacts due to insufficient defenses [3]. Wealthier nations also tend to adopt comprehensive national cybersecurity strategies, further improving their resilience against threats [6][9].

Digital Literacy

Awareness campaigns targeting vulnerable groups, such as children and small businesses, have proven effective in reducing the success rates of cyberattacks. Programs aimed at child online protection are active in 94 countries, contributing to a noticeable reduction in exploitation risks [1][4]. Digital literacy initiatives also improve the security posture of smaller enterprises and communities, enabling better identification and response to cyber threats [7][10].

This analysis highlights the importance of demographic factors in shaping a nation's cybersecurity posture and resilience, underscoring the need for targeted education and infrastructure investments to address emerging cyber risks [11][12]. Ensuring that a policy can be met by the capabilities of a nation's infrastructure ensures that there isn't a gap between what a nation wants to implement and what they are capable of implementing.

Validation of Theory

Key Findings

Countries in GCI Tier 1, such as Singapore, consistently implement policies that adress all five pillars effectively, resulting in reduced frequency and impact of cybercrimes. For example, Singapore's comprehensive approach to capacity building and international cooperation has set a global benchmark [1][4]. When a nation is constantly aware of where they stand in terms of meeting cybersecurity benchmarks and more importantly their own needs as a country, they are able to implement the most effective policies. The most effective policies tend to be ones that are up to date with current technologies, ensure a

transparent and efficient use of handling data, as well as properly securing critical infrastructure and educating groups so they are aware of how to be safe from cyberattacks.

Lower-tier countries show significant gaps in technical and capacity-building measures, highlighting areas for prioritized improvement [3]. Learning from the mistakes and progress of model nations such as Singapore and developing proper policies that address the growth of their nation as well as the budget constraints that they face will allow them to grow at a steady rate and mitigate risks from adversaries.

Limitations and Recommendations

Limitations

Data Gaps

The inconsistent reporting of cybercrimes globally presents significant challenges for comparative analysis. Many developing countries lack standardized reporting mechanisms, making it difficult to assess trends and draw actionable conclusions [3]. Additionally, gaps in real-time data collection hinder the global monitoring of cyber threats, as reported in various studies [5][6].

Dynamic Threat Landscape

The rapid pace of technological advancements, such as AI and quantum computing, means that cybersecurity policies can become outdated quickly. These technologies introduce new vulnerabilities and attack vectors that require constant adaptation of policies and defense strategies [4][9]. As a result, cybersecurity frameworks need to be agile enough to accommodate emerging threats [8].

Policy Implementation

Differences in political will and resource allocation across regions continue to hinder the uniform application of cybersecurity policies. While some nations prioritize cybersecurity through investment and national strategies, others face challenges due to political instability or lack of resources, resulting in inconsistent policy implementation [3]. This disparity is also reflected in the global diversity of cybersecurity maturity levels [7][12].

Recommendations

Enhance Data Sharing

Establish global open-access databases for cyber risk and incident reporting to improve transparency and coordination. This would enable nations to share real-time data and

analysis, enhancing global awareness and response capabilities. Existing frameworks, such as public-private partnerships in 108 countries, demonstrate the value of sharing cyber intelligence [1][4].

Invest in Education

Implementing policies that expand cybersecurity education programs to cover all levels—from primary to professional education. Nations that have integrated cybersecurity curricula, such as Finland, have seen tangible reductions in human-error-related incidents and an overall boost in national cybersecurity resilience [1][4]. Widespread education programs can cultivate a more informed and vigilant society [10].

Strengthen Cooperation

National policies that utilize international partnerships with a focus on capacity building for lower-tier nations. By supporting cybersecurity initiatives in developing countries, global cooperation can help reduce vulnerabilities and promote a more unified approach to cybersecurity. International collaborations, such as those seen in public-private partnerships, have proven effective in strengthening global cybersecurity defenses [4][8].

Continuous Policy Review

Regularly update policies to address emerging threats, leveraging feedback from cyber audits, real-time data analysis, and global trends. Cybersecurity is a continuously evolving field, and governments should ensure that their policies remain adaptive by incorporating feedback from international forums and cybersecurity experts [3][4]. A proactive approach will help keep pace with the rapidly changing threat landscape and maintain effective defense systems [9].

By addressing these limitations and pursuing the outlined recommendations, we can build a more resilient global cybersecurity ecosystem that can adapt to emerging challenges.

Proposal

After analyzing the data above and gathering conclusions based on multiple data points from various regions and looking at how policies are implemented effectively and ineffectively as well as cybersecurity standards, the most effective national cybersecurity

policies are those that adhere to basic cybersecurity standards meeting frameworks such as NIST and CIS as well as adapting policies to fit the nations specific needs. Nations in

lesser developed areas should focus on adopting policies that allow continual growth of their technology while ensuring the security of critical infrastructure and maintaining security standards that can be met by their budget. Some examples of these would be policies that ensure up to date maintenance of technology ensuring the most recent patches are put in place or a policy that requires a set amount of training scenarios/learning modules to take place to ensure up to date knowledge for the public and the technology community of the nation. Policies that enable collaboration with welldeveloped nations should also be a focus as they have the knowledge, experience and resources to assist with the cybersecurity of a lesser developed nation. For the nations that are already well established as role models or mid-tier countries in terms of cybersecurity posture, it is critical to maintain the current upkeep of policies while also ensuring up to date policies that address current threats and vulnerabilities to the nation. Similarly to the lesser developed countries, enacting policies that ensure the security of critical infrastructure and Research and Development projects is very important. Well developed countries such as the United States, Russia and China are also huge targets for each other and thus should enforce policies that address nation-state attacks and the severity that one can have on the nation as well as a plan for if a major breach were to occur. Outside of the general policy enforcement each nation should address its current state of cybersecurity and technology as well as its goals for the future, budget, technological capabilities and current policy structure and compose tailored policies that address the individual nations state of cybersecurity and allow it to mitigate the attack surface for bad actors as much as possible.

Conclusion

Strong national cybersecurity policies rest on a combination of legal, technical, organizational, capacity-building, and cooperative measures. Data-driven analysis of global cybercrime distribution and national strategies provides actionable insights for policy refinement. By addressing identified gaps and fostering international collaboration, nations can enhance their cybersecurity posture, reduce vulnerabilities, and build resilience against evolving threats.

Problem Chosen F	2025 MCM/ICM Memo	Team Control Number 2500778

To: ITU Summit National Leaders

Subject: Advancing National Cybersecurity through a Multilevel Policy Framework

The growing presence of both sophisticated and simple cyber threats requires a comprehensive and adaptive approach to national cybersecurity. These threats pose significant risks to government operations, economic stability, and public trust. Drawing insights from the Global Cybersecurity Index 2024, and other data sources and compliance frameworks this memorandum emphasizes the need for a multilevel cybersecurity policy approach that combines universal protections with tailored national solutions, considering the unique sociopolitical, economic, and technological situations of different nations.

National cybersecurity efforts must prioritize clear and enforceable legal and regulatory frameworks. While 91% of countries have adopted cybersecurity laws. These laws should align with international standards like the GDPR and be applied across jurisdictions to enhance foreign collaboration. Technical measures are equally critical, yet only 72% of countries have operational Computer Incident Response Teams (CIRTs). Expanding CIRT capabilities, integrating them into regional networks, and conducting regular joint cyber drills will strengthen national and regional cyber readiness.

Collaboration is another key component, yet only 63% of countries currently participate in public-private partnerships (PPPs). Governments should prioritize establishing PPPs and enhancing international cooperation for intelligence sharing and capacity building. This collaborative approach will bolster resilience against foreign adversarial threats.

Considering the ever-changing cybersecurity landscape, national leaders are urged to adopt a multilevel policy framework that adopts enforceable legal standards, enhances technical capabilities, integrates adaptive organizational strategies, expands the current state of technology, and fosters both domestic and international cooperation. Cybersecurity is a shared challenge that demands a unified and proactive response. By implementing this tailored approach, nations can safeguard their digital ecosystems while contributing to a globally resilient cyberspace.

Problem Chosen F	2025 MCM/ICM Reference Page	Team Control Number 2500778

[1] "Global Cybersecurity Index 2024." https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 (accessed Jan. 25. 2025).

[2] "Cyber Governance Studies" https://doi.org/10.1365/s43439-021-00045-4 (accessed Jan. 25. 2025).

[3] "Cyber Risk and Cybersecurity" https://doi.org/10.1057/s41288-022-00266-6 (accessed Jan. 25. 2025).

[4] National Cybersecurity Guide - Good Practice: https://ncsguide.org/the-guide/good-practice/ (accessed Jan. 26. 2025).

[5] "Visual Analytics for Cyber Security Domain: State-of-the-Art and Challenges" https://link.springer.com/chapter/10.1007/978-3-030-30275-7_20 (accessed Jan. 26. 2025).

[6] "Federal Bureau of Investigation Internet Crime Report" https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf (accessed Jan. 26. 2025).

[7] "CISA Through the Years: Policy and Impact" https://www.cisa.gov/news-events/news/cisa-through-years-policy-and-impact (accessed Jan. 26. 2025).

[8] "Exploring National Cyber Security Strategies: Policy Approaches and Implications" https://www.rusi.org/explore-our-research/publications/occasional-papers/exploring-nationalcyber-security-strategies-policy-approaches-and-implications (accessed Jan. 26. 2025).

[9] "Developing Robust Cybersecurity Policies and Governance Frameworks in Response to Evolving Legal and Regulatory Landscapes" https://ieeexplore.ieee.org/document/10687438 (accessed Jan. 26. 2025).

[10] "Pioneering Security in the Quantum Era: Preparing Travelers Insurance for a PostQuantum Future" https://blackpenguin46.github.io/quantum-paper/ (accessed Jan. 26. 2025).

[11] "CYBERTHREAT LIVE MAP" https://cybermap.kaspersky.com/ (accessed Jan. 26. 2025).

[12] "Developing countries most vulnerable to cyberattacks" https://news.un.org/en/story/2011/12/397922 (accessed Jan. 26. 2025).

[13] "Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024" https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usdannually-in-2024 (accessed Jan. 26. 2025).