Influence of Public Perceptions on Cybersecurity Policy Framework Formation

Johannes Joubert and Mike Wa Nkongolo
University of Pretoria, South Africa

u20582006@tuks.co.za
mike.wankongolo@up.ac.za

Abstract: This systematic literature review seeks to understand influence of the relationship between public perceptions and governmental responses to cybersecurity. The focus is on how these perceptions influence policy formulation processes. This is achieved by comparing the approaches of the United States of America (U.S.A), China, Australia, and Sweden. We analyse the alignment and discrepancies between public expectations and governmental cybersecurity strategies. And examine the legislative and practical challenges of bringing public views into play within effective policy frameworks. While the findings highlight high public awareness and concern about cybersecurity, the analysis appears to overly generalize without considering disparities in public awareness across socio-economic groups or regional variations, raising questions about the representativeness of these conclusions. What we reveal across governance models is a common tendency for reactive rather than proactive governmental responses with differing degrees of openness and public participation. Hence, a conclusion is drawn on the proposal of a theoretical framework that would promote a participative approach to policymaking in cybersecurity between governments and the public. A policy which enhances its relevance and effectiveness by being resonant with the public's concerns and global standards. This policy serves as the foundation for robust, practical, and highly inclusive cybersecurity frameworks designed not only to address technological threats but also to align with public expectations and perspectives on national security.

Keywords: Cybersecurity framework, Public perceptions, National security, Policy formulation, Cyber attacks

1. Introduction

Social media platforms are integral to modern life, with most human activities requiring an online presence. Cyber threats are more prevalent than ever, risking personal information and national security. Advancing cyber-attacks heighten public concern about cybersecurity (Snider et al., 2021). Governments face rising pressure to protect critical infrastructures and citizens from online threats. Despite increased demand, there is limited understanding of how cybersecurity threats influence political decision-making and policy development. Labelling countries as reactive oversimplifies policy dynamics, as factors like resource constraints or geopolitical pressures may necessitate reactive measures (Gandhi et al., 2011). We will examine how public perceptions of cybersecurity influence political decision-making and policy formulation. The literature review explores the relationship between public perceptions and policymaking, assessing whether public input benefits cybersecurity policies. The study proposes a theoretical framework for inclusive and secure policymaking, aiming to bridge the gap between public opinion and government action on cybersecurity.

2. Background

Cybersecurity policy formulation varies by country, but universal fundamentals exist. This literature review aims to gather public and governmental perspectives on cybersecurity to address these fundamentals. The review followed a PRISMA model, identifying 360 records via database searches. These databases include but are not limited to Web of science, Sage, IEEE Xplore and EBSCOhost. Duplicates were removed, leaving 348 records. Screening is also implemented to eliminate papers based on inclusion/exclusion criteria. The criteria included non-English papers, inaccessible papers, and unpublished articles. This reduced the count to 89 articles. After assessment, 58 articles were excluded, leaving 31 for synthesis. This process can be seen in Figure 1.

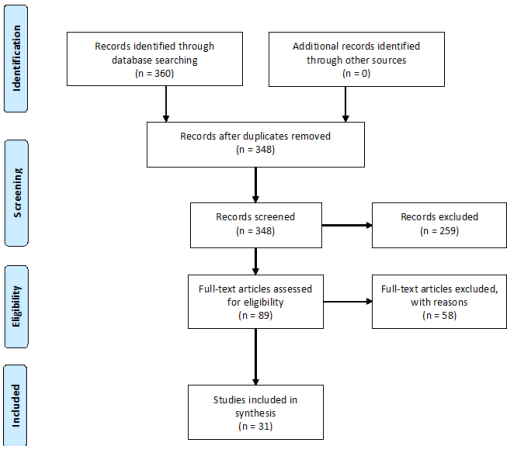

Figure 1: PRISMA flowchart

All articles included in this synthesis were analysed, and the following attributes were extracted from each paper: Publication year, Topic discussed, and Themes. This data is collected for 31 articles, and a grouped bar chart is constructed to visualize the co-occurrence of topics (see Figure 2 x-axis) and themes (see Figure 3 x-axis) found within the document bodies. The shared x-axis categories represent common cybersecurity themes and topics in Figure 2 and 3. This visualization allows for the exploration of potential relationships between public framing of cybersecurity issues and the focus of policy discussions within the documents.

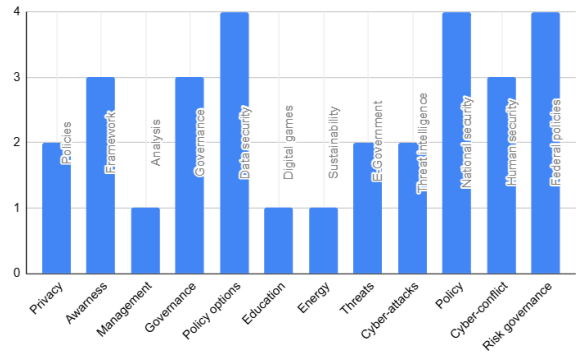

Figure 2: Cybersecurity topics

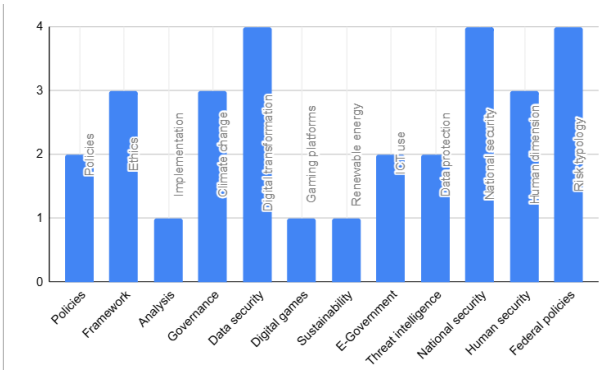

Figure 3: Cybersecurity themes

Analysis of Figure 2 reveals several notable associations. For example, the high bar for "National Security" combined with "Policy" suggests that documents with a focus on national security frequently discussed policy concerns. National security is a prominent theme carrying in titles as seen using “Federal”, “Government” and “National” which shows it is a main point for researchers to target. Figure 3 presents further insights. It suggests correlations between "Data Protection" with "Privacy," "Ethics," "Data Security," and "Human Dimension". This suggests that public attention to data protection is strongly linked to policy discussions incorporating privacy considerations, ethical guidelines, data security measures, and the human impact of cybersecurity policies. The presence of "Policies" related keywords across multiple high bars shows the importance of policy frameworks to the broader spectrum of public cybersecurity concerns. Upon further review of preliminary findings, a significant limitation is the difficulty in accessing complete and direct information on governmental cybersecurity strategies. Highly regulated countries and papers relating to them have a somewhat distorted view on the implications of policies. This indirectly affects the relevance of findings because some countries do not have enough timely information to draw conclusions from. Very few countries are well researched on public cyber warfare (Gandhi et al., 2011). For the above-mentioned reasons, the only countries that are represented in this review is the United States of America (U.S.A), China, Australia, and Sweden. According to the preliminary investigations these four countries are very diversely structured with a broad variety of cybersecurity approaches and have enough research to back claims. The exclusion of nations from Africa, Latin America, and Southeast Asia risks overlooking innovative, context-specific approaches to cybersecurity policies but do not provide enough sources to make an accurate example. A comparative analysis will be used to find common themes and trends on what works for policy formulations. This will aid us in building a cohesive policy framework based on international standards to meet public expectations.

3. Findings

This literature review first examined the current state of public involvement in government policy creation. It then highlighted differences in cybersecurity understanding between the public and governments. The study examined the perspectives and regulations guiding both groups to see how governments address cybersecurity. The findings are structured as follows: first, public, governmental perceptions, and approaches to cyber policies are explored, followed by a comparative analysis of multiple countries. Finally, a proposal of the hypothetical framework was the best conclusion that could be reached. This ensured that public will be adequately involved in the policy creation.

3.1 Current Public Involvement in Cybersecurity Policies

The 2022 Deloitte–NASCIO Cybersecurity Study and the Eurobarometer 2024 report reveal that public input into government cybersecurity policy frameworks is fragmented and underdeveloped (Rupp, 2024). Governments have implemented frameworks like the EU's NIS Directive and U.S. state-level policies, but these often lack mechanisms for meaningful public engagement or adaptability in the evolving cybersecurity landscape. The complexity of the newer online policies leaves the public out due to a perceived lack of knowledge around international digital security needs. This, along with numerous new IT security policies, shows a bleak picture of public participation in cybersecurity policies (Figure 4).

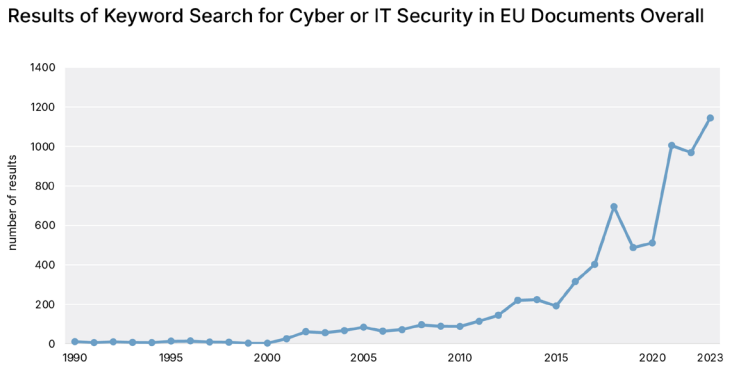

Figure 4: The usage of the words 'IT Security' and 'Cyber security' in EU documentation (Rupp, 2024)

The Deloitte–NASCIO study highlights structural barriers like insufficient agency coordination and slow integration of innovative approaches (Subramanian and Ward, 2022). Both studies suggest that despite growing public awareness of cybersecurity risks, there is a pressing need for participatory, transparent, and flexible frameworks to incorporate public priorities and address emerging threats.

3.2 Public Views on Cybersecurity

There has been a significant surge in public awareness of cybersecurity risks in recent years. Coenraad et al. (2020) advocate for gamified learning but do not examine whether it provides deep understanding or merely superficial awareness. They state that the popularity of games involving acquiring and using other players' details indicates awareness and concern about cybersecurity. Snider et al. (2021) attribute heightened public concern to media exposure but do not assess whether media narratives exaggerate risks, leading to disproportionate public fears. They show that people more conscious of cyber threats likely consider them significant risks.

Choudhury et al. (2021) show that comprehensive educational initiatives can significantly improve the public's ability to recognize and respond to cyber threats. This ties in perfectly with trust issues the public is currently having. Coenraad et al. (2020) indicates a lack of trust in institutions managing cybersecurity. This is mostly due to digital games reflecting the contemporary fears and worries of society about data security. Although low public trust is highlighted, this perception might differ significantly across demographics, suggesting the need for a nuanced analysis of trust drivers beyond general assertions. Snider et al. (2021) proposes that exposure to cyber threats by individuals creates tendencies for low trust not only in government but also in corporate cybersecurity practices. This in return creates the need for clear and effective cybersecurity policies among the public to restore trust. The cry by the public for more protective measures and policies that are clear and persuasive than ever. It is as a result of this that game designers propose robust practices (Coenraad et al., 2020). Snider et al. (2021) also noted that there is a great chance of regulatory support for strict rules on

cybersecurity by individuals who have experienced cyberattacks. Their study insinuates that there is a public call for regulation policies and transparency in the control of cybersecurity threats. This growing support of regulatory actions only attests to the fact that the public desires solid and all-encompassing policies on cybersecurity.

3.3 Government Views on Cybersecurity

The world's interest in considering cybersecurity as one of the primary components of national security has been growing. Governments have demonstrated this level of importance in their policy papers and speeches (Carr and Lesniewska, 2020). Among the reasons cybersecurity policies are pursued is due to increased pressure for national security. For example a serious turn toward examining cybersecurity came in the light after Russia's aggression against Ukraine in 2014 which brought forth significant policy transformations in Lithuania in 2017-2018 (Vilpišauskas, 2024). Ghandi et al. (2011) also showed that critical infrastructures - water, electricity, healthcare, finance, and transportation - are becoming ever more software dependent and interdependent making them at greater risk now than ever before in history from attacks launched through cyberspace as part of political or social unrest. If we can look into research conducted by Asllani et al. (2013) they provide insights into the ways governments are currently securing digital transactions and critical cyber infrastructure. Their research concluded that effective cybersecurity frameworks are essential for the protection of digital transactions and critical infrastructure, ensuring both national security and economic stability. Besides this there is a trend in most governments that their reaction to cyber problems has been more reactive than proactive. While Vilpišauskas (2024) links Lithuania's cybersecurity transformation to external geopolitical pressures, this overlooks whether domestic factors, such as public advocacy or local institutional changes, also contributed to these policy shifts. This reactive approach points to the lack of understanding and attention paid to issues related to cybersecurity initially by policymakers until substantial political pressure is created. Ghandi et al. (2011) finds that it also explains the reaction across the globe to cyber-attacks. In most instances, only after a problem was registered action was taken. They therefore argue that current models of anomaly detection focus on the analysis of network traffic in the prevention of malicious activities and not taking into account the human behaviours that cause such anomalies. Behaviours that are often influenced by social, political, economic, and cultural conflicts at large (Gandhi et al., 2011). Certain governments are putting up impressive levels of investment in cyber infrastructure as well as education. The paper by Dehghani et al. (2023) prioritizes technological evolution but overlooks the socio-political challenges of adopting new measures, particularly in nations where public mistrust or political resistance could hinder implementation. Vilpišauskas (2024) also mentions incidents in the Lithuanian cyberspace investment. This sector grew to the greatest extent but Vilpišauskas (2024) fails to mention that the Lithuanian government was lagging behind due to negligence. After 2017 policy and institutional frameworks passed through a sweeping change in Lithuania. Ghandi et al. (2011) looked into the financial sector and its efforts and challenges associated with cybersecurity. They concluded that countries that make proactive investments toward security measures makes them less prone to cyber-attacks. These investments increase anomaly detections, enhance public-private cooperation, and promote education through training programs and the creation of an expert cybersecurity workforce (Gandhi et al., 2011). Investment in cybersecurity is also being shaped by strategic cybersecurity initiatives that align with broader national security strategies. Widjaja (2023) highlights how these strategic initiatives are critical for sustaining long-term security and economic stability, as they are designed to not only respond to immediate threats but also to anticipate future challenges in the cybersecurity landscape. From a government perspective they need to consider the legal frameworks that impact and govern these policies as well. Although legal frameworks establish enforcement mechanisms, their rigidity may hinder adaptability to rapidly evolving cybersecurity threats, potentially creating gaps in protection as highlighted by Kosseff (2020). According to Kossef (2020) these frameworks are critical for defining the roles and boundaries of public and commercial organizations in the cybersecurity sector. While Kosseff (2020) emphasizes the importance of legal frameworks, the study lacks discussion on how these frameworks might lag technological advancements, creating gaps in enforcement and compliance.

3.4 Comparative Analysis of International Approaches

It is clear what aspects of cybersecurity are considered relevant by both governments and the public. This section looks at how these requirements are considered in practice within some countries as examples (Figure 5). It looks at their specific political and social environment as frameworks to practice cybersecurity. And investigates the ways in which cybersecurity policies come to be nationally and the connections between the actions of governments and citizens' input. Figure 5 presents a general idea of the security level pertaining to

each country together with their government structures from the preliminary investigations. This comparative analysis is important because different national contexts are shaped by cultural, economic, and political factors and impact the formulation and implementation of cybersecurity policies (Kshetri, 2020). Before delving into the specific policies of the individual countries one first need to understand where all of them are politically as well. The political leaning is grounded on how the government is structured which is displayed in Figure 5. Additionally, the section discusses governmental structures regarding cybersecurity to help us understand why various countries have specific policies as portrayed in Figure 5. This is important because as Carr and Lesniewska (2020) states, cybersecurity policies are heavily influenced by the political framework and the governance model of a country (Figure 5).

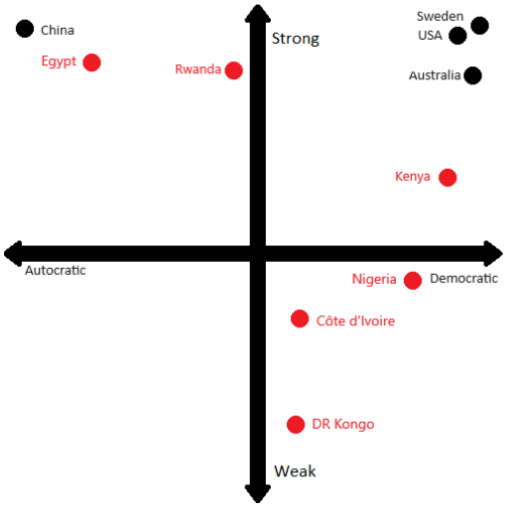

Figure 5: Governmental structure to security strength matrix

United States of America (U.S.A)

The U.S.A, a democratic nation with a federal government (Figure 5), has embedded cybersecurity in its national security framework through public-private collaborations and legislative interventions. This multi-faceted approach is due to the decentralized nature of the U.S. government, allowing varied and sector-specific cybersecurity policies. According to the Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency (CISA) leads cyber defence information exchange and collaboration among federal, state, local, tribal, and territorial governments, the private sector, and international partners. CISA has two primary operational functions. First, CISA leads federal cybersecurity, protecting and defending federal civilian executive branch networks in partnership with the Office of Management and Budget, the Office of the National Cyber Director, and federal agency CIOs and CISOs. Second, CISA coordinates critical infrastructure security and resilience, working with government and industry partners. The U.S. government is updated on cybersecurity threats and has a dynamic legislative and strategic approach. Sivan-Sevilla (2021) claims that these policies' applicability depends on public and private sector support, highlighting the importance of private actors in cybersecurity.

China

China, under a centralized and authoritarian regime, has a strict and constantly monitored approach to cybersecurity (Figure 5). The Cyberspace Administration of China (CAC) tightly regulates internet traffic (Li et al., 2022). The CAC is involved in the formulation and implementation of policy on a variety of issues related to the internet in China. It is under direct jurisdiction of the Central Cyberspace Affairs Commission, an institution subordinate to the Chinese Communist Party (CCP) Central Committee. Internet freedom is substantially restricted, and the state closely monitors all activities on media and technology networks and has elaborate legal frameworks to safeguard national security. Li et al. (2022) emphasize China's control-oriented model but fail to explore whether this approach sacrifices innovation and adaptability, especially as rigid control could hinder private sector contributions to cybersecurity advancements. The public perception of cybersecurity is a result of state discourse that promotes the importance of extensive governmental control against threats originating from abroad, internal traitors, and enemies. Although there is a deep focus on control, all areas of cybersecurity are well regulated and up to international standards (Li et al., 2022).

Australia

Australia, a liberal democratic country, mainstreams both cyber power and democracy assurance in its cybersecurity approaches (Figure 5). According to the Australian government, this resilience system is directly linked to their Australian Cyber Security Strategy that stretches from 2023 to 2030. The Department of Home Affairs oversees developing and coordinating the Australian Cybersecurity Strategy. This department is largely responsible for developing and implementing Australia's cybersecurity legislation and policies. To improve the country's cybersecurity reach, the Department of Home Affairs works with various governmental and non-governmental organizations, including the Australian Cyber Security Centre (ACSC). The ACSC is overseen by the Australian Signals Directorate, which provides cybersecurity guidance and assistance, influencing government policies and strategies. A survey conducted by Manwaring and Holloway (2023) in Australia revealed that the public is very sensitive to cyber threats or cyberattacks, especially those linked to foreign interference in the country's political affairs. Manwaring and Holloway (2023) frame resilience as a strength but neglect to evaluate whether top-down resilience strategies marginalize grassroots and local efforts to combat cyber threats. The Australian government has been highly reactive in this area, subsidizing significant investments directed towards the field. Australia remains committed to strengthening both its technological capabilities and democratic processes to counteract cyber threats (Manwaring and Holloway, 2023).

Sweden

The Swedish political system is democratic with a great focus on people's involvement in governmental processes, and like any other nation globally, they have adopted specific models on cybersecurity policies (Figure 5). According to the Swedish national cybersecurity strategy, the Swedish Civil Contingencies Agency is responsible for coordinating national cybersecurity efforts. The Swedish government designs and implements the entire cybersecurity plan and uses a regulatory framework to enforce this. The regulatory framework includes the Protective Security Act, as well as European Union rules such as the General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS) directive. Other authorities are also included in this comprehensive framework. For instance, the Swedish Armed Forces and the Swedish Post and Telecom Authority (PTS) have specific regulatory and enforcement responsibilities to ensure a strong and compliant cybersecurity infrastructure across the country (Yusif et al., 2024). Yusif et al. (2024) praise Sweden's participatory model but fail to address potential blind spots, such as whether public participation effectively influences policy or merely serves as symbolic inclusion without substantial impact. The government does not perceive cybersecurity solely as a technical domain but also social, incorporating citizens in its determination and implementation processes. The attitude of Swedes towards actions and programs carried out by the government in cybersecurity is positive due to the high level of trust towards institutions in Sweden. The government is protective and proactive, practicing constant innovation in its approaches to combat threats from innovative technologies. This has vested in higher resilience and sound policies regarding cybersecurity in Sweden (Yusif et al., 2024).

3.5 Policy Formulation Process

The major activities in the formulation of cybersecurity policies encompasses the identification of the issue, consultation, and policy implementation response (Asllani, 2013). In the United States, the federal government has set an elaborate structure of policies that guide the formulation of cybersecurity policies. As indicated by Sivan-Sevilla (2021) this begins by identifying vulnerabilities and risks, especially in areas of utmost importance. Policy makers apply several layers of consultations with various stakeholders, including government policy makers and agencies, private sector, and NGOs. This prevents situations when poorly thought-out policies might be implemented due to pressure in one team but did not consider the shared goals of the organisations (Sivan-Sevilla, 2021). The last steps are to write them into laws and introduce them in as acts and pass them through the parliament and to apply them in various sectors. Similarly, China's policy formulation is considered a highly centralized procedure, with a limited number of policymakers given the authority to decide on policies and their implementation. According to Li et al. (2022), the Chinese authoritative agencies and institutions are the primary actors informing the Chinese government of cybersecurity concerns. A lot of input from top governmental officials and experts exists when determining the formulation of policies often with a primary objective of enhancing national security. While the authoritarian system in China limits public consultations, this absence could also reflect a deliberate strategy to maintain state control over sensitive cybersecurity issues, which merits further exploration of its trade-offs compared to democratic systems. Policies are swiftly implemented across all levels of government, ensuring uniform adherence and enforcement. Lithuania's is an example where external shocks accelerated policy development.

Vilpišauskas (2024) notes that the Russian aggression against Ukraine fueled comprehensive policy changes in Lithuania. Initially, the policy development process was slow due to limited understanding and resources. However, the increased geopolitical threats prompted a more urgent and coordinated response, leading to the establishment of a robust cybersecurity framework (Vilpišauskas, 2024).

3.6 Policy Creation Restrictions

Nkongolo (2023) identified strategic challenges in cybersecurity policy formation. He noted the lack of clear global standards complicating the harmonisation of national policies with international expectations. He emphasises the need for a strategic framework that not only addresses the immediate security requirements but also ensures compatibility with evolving global cybersecurity norms.

3.7 Stakeholder Engagement

In all discussed articles where a good policy creation process is followed, the importance to manage stakeholders was mentioned. When developing policies - especially on those concerning cybersecurity - it involves many players. According to Sivan-Sevilla (2021) it supports public-private partnership in which technology players and companies that manage and own critical infrastructures work together with the government departments to come up with the frameworks of cybersecurity and their execution. While public-private collaborations are positioned as effective, they often prioritize corporate interests, potentially marginalizing the public's role in shaping cybersecurity priorities. Furthermore, the other countries in this analysis have open relations with stakeholders. China exercises more authoritarian approach to stakeholder relations (Figure 5). Li et al. (2022) state that the Chinese government consults with a limited number of individuals, many of whom represent state-owned undertakings and government organisations. The engagement process is hierarchical and dominated by government, with minimal participation from the citizens and no participation by independent voices. Enhanced policy compliance is possible because this model entails stricter adherence to prescribed legislation but lacks a multi-faceted approach that enriches laws and policies.

3.8 Standards and Compliance

Cybersecurity policies are subject to numerous standards and compliance set by the nation as required by international law as well as legal systems. In the case of the U.S.A, local law enforcement as well as the federal laws along with the guidelines of public bodies like the National Institute of Standards and Technology (NIST) influence these processes (Sivan-Sevilla, 2021). The U.S.A policies have been oriented to providing security response solutions that are compliance with high-level security challenges. Compliance is monitored through regular audits and assessments, ensuring that entities adhere to established protocols (Sivan-Sevilla, 2021). Standards and compliance in China are tied with stronger roots to the nation’s security strategy than is the case in the U.S.A. The Chinese government has very high cybersecurity standards which it applies towards its aim of controlling societal activities and protecting the state (Li et al., 2022). It is also rule-based, this is complemented by tough regulatory measures against non-compliance. While this approach offers maximum security, the levels of flexibility and innovation that such configurations can offer are limited (Li et al., 2022). Although not part of the comparative analysis, Lithuania is a good example of standards that change for the good. The evolution of cybersecurity standards in Lithuania has been significantly influenced by international norms and the need to align with EU and NATO requirements. Vilpišauskas (2024) explains that Lithuania's cybersecurity policies are designed to meet both national security needs and international standards. This dual focus ensures that Lithuania remains compliant with global best practices while addressing specific national threats. The integration of international standards has also facilitated greater cooperation with other countries and international organizations (Vilpišauskas, 2024). After looking at various countries and stakeholders in cybersecurity policies, we propose a Venn diagram to understand what concerns are related to every stakeholder and what every stakeholder will consider most important (Figure 6). With this in mind the study will now look at how to come up with a framework that supports all stakeholder needs.

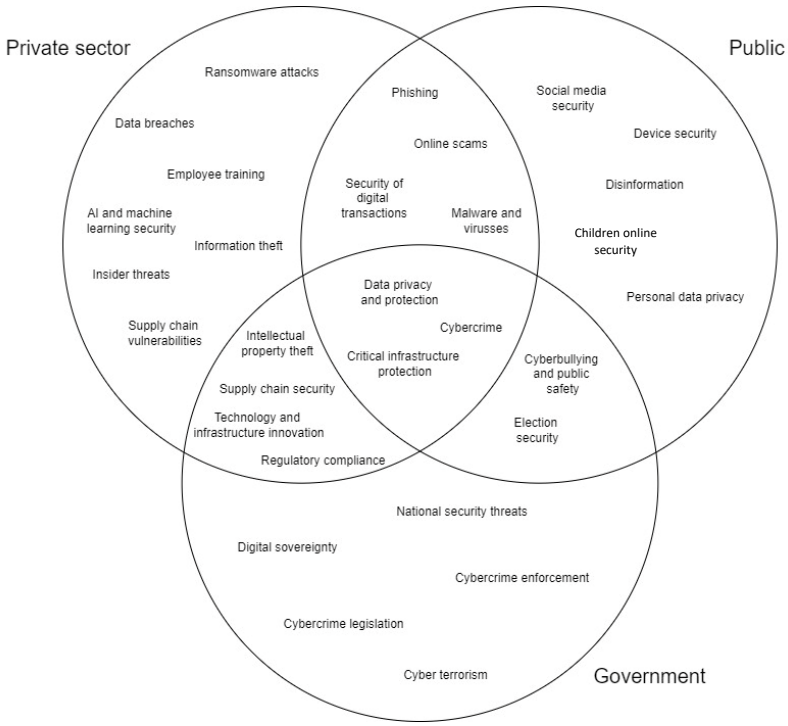

Figure 6: Stakeholder correlation Venn diagram

3.9 Policy Framework Based on Analysis

This section develops a cross-cultural, data-driven framework for international cybersecurity policymaking, by analyzing stakeholder roles and political constraints.The section proposes the framework adapted for varied global needs.

Proposed Cyber-Policy Framework

The idea of this framework is to involve various stakeholders affected by cyber-attacks to develop the best policies. Such stakeholders include governments, private sectors, and public sectors. They should all be involved in policy formulation of cybersecurity. Governments should introduce key strategic vision and strong regulatory approaches (Vilpišauskas, 2024), while the private sector should bring innovations and implementation expertise (Sivan-Sevilla, 2021), and the public's role is to remain informed and active, so that the policies are relevant and sensitive to values shared amongst citizens (Snider et al., 2021). This collaborative approach is crucial for developing resilient and adaptive cybersecurity policies that can respond to dynamic threats. The proposed framework can be divided into four distinct components, each representing critical elements: Threats, Targets, and Defences (Figure 7). The "Threats" component, positioned at the top, identifies potential risks that must be addressed to mitigate cyber vulnerabilities (Figure 7). The "Targets" component focuses on industries or sectors likely to be targeted, emphasizing the potential for these attacks to destabilize the country (Figure 7). On the left, the "Defences" section outlines the collaborative measures undertaken by the public and private sectors to prevent threats from reaching the identified targets (Figure 7). On the right, the governmental approach is represented, highlighting the state's strategic role in countering cyber threats (Figure 8). The intersections between these sections reflect the interconnection and inter-dependencies among them, emphasizing areas where collaboration is essential. This framework is designed to visually illustrate the shared responsibilities of the public, private sector, and government in ensuring cybersecurity. It provides a structured overview of the priorities and considerations deemed critical for national security (Figure 8).

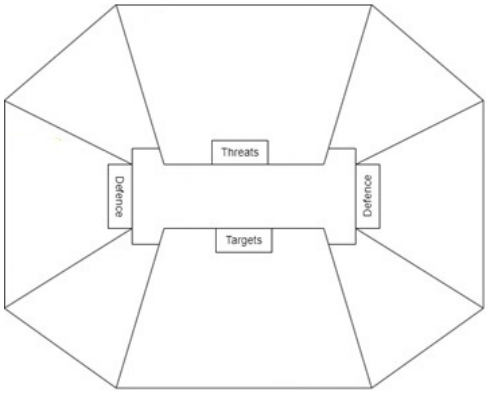

Figure 7: Framework's components

Moreover, it serves as a flexible tool, allowing countries to assess their cybersecurity strategies and verify whether their existing measures comprehensively address all key aspects of protection. To apply this framework in practice, the study uses South Africa in 2024 as a hypothetical test case (Figure 8).

South Africa Approach to the Proposed Framework

South Africa is an ideal example for applying this framework, particularly in 2024 due to it being a critical election year. The socio-political significance of the elections makes the country a prime target for cyber threats like misinformation, data breaches, and attacks on electoral systems (Figure 8). Figure 8 highlights key threats, targets, and defences tailored to South Africa's needs which includes electoral measures. South Africa's cybersecurity policies is inspired by international frameworks from the EU, NATO, and the U.S.A which makes it a strong universal candidate. South Africa uses the National Cybersecurity Policy Framework (NCPF) which directly copies ideas from the aforementioned entities (Sutherland, 2017). This adaptable framework can guide other countries in addressing their unique cybersecurity challenges.

South Africa Analysis

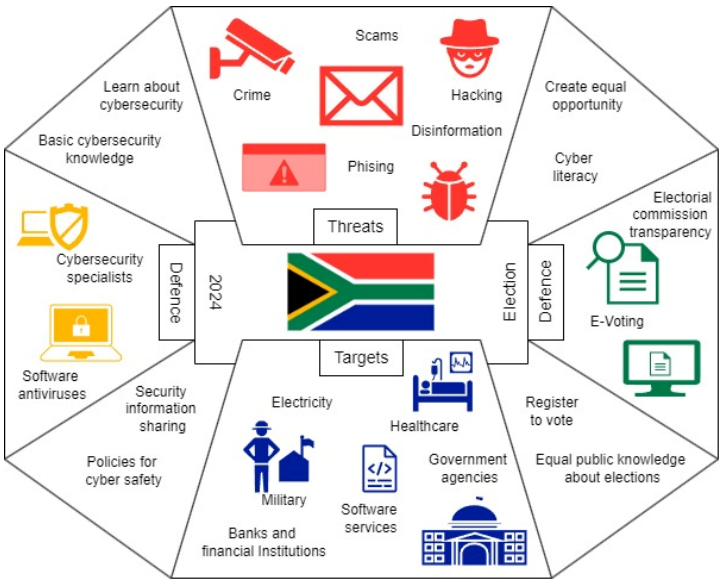

Figure 8: South Africa approach to the framework in 2024 election

South Africa's diversity of priorities is reflected in its framework by identifying critical targets, showcasing the country's multifaceted nature and its need for robust cybersecurity policies. These targeted areas are likely similar in other nations, making South Africa a good comparative example. However, the current NCPF has been criticized for adopting international strategies too quickly, creating potential vulnerabilities rather than advantages (Sutherland, 2017). South Africa's example is also influenced by its election year, as threats evolve with time, suggesting frameworks should be updated annually. Additionally, the framework overlooks the existing security of targets, which must be addressed to ensure completeness in future iterations (Figure 8).

Proposed Framework Structure

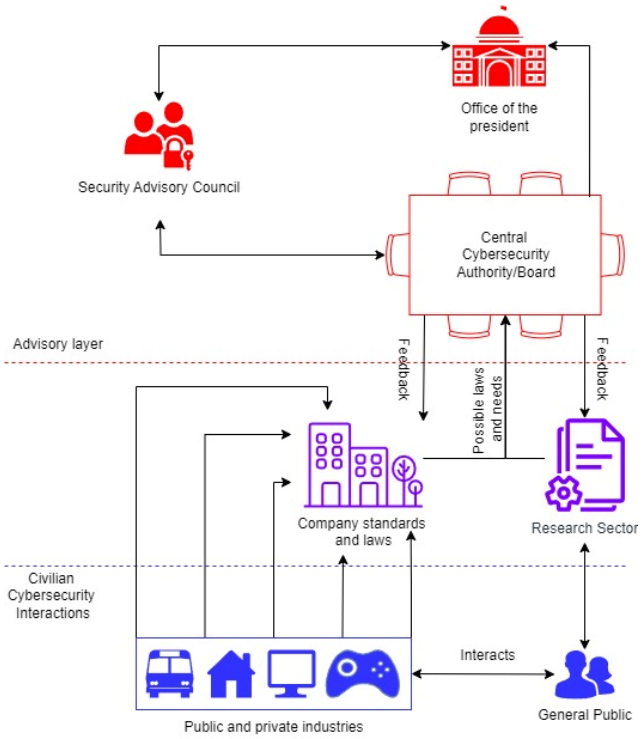

Figure 9: Governmental structure of the framework

The governmental structure that utilises the proposed framework is illustrated in Figure 9 (Mugisha, 2019). The structure is broken down in an advisory and civilian cybersecurity interactions layer (Figure 9). Firstly, in the direct interactions layer, the public feeds various private and public sector companies. The advisory layer is where new cybersecurity laws are created. This layer also feeds into the office of the president to ensure laws are up to date and relevant. This layer receives input from the relevant public and private sectors as well as the research division that would keep up to date with trends and needs. This is achieve to ensure that if needs are missed by the public and private sector that it will not go unnoticed. Part of the advisory layer there is a Security Advisory Council to ensure laws stay compliant and align with national goals. Figure 9 shows the government structure to enforce ideal cybersecurity policies via the proposed framework.

Limitations of the Framework

There are some limitations to the proposed framework. There are numerous types of governmental systems, this framework cannot work for some of the countries that are autocratic with limited public participation in policy making as is shown in the China analysis (Li et al., 2022). In such cases more focus may be placed on the role of international pressure and the obligations that stem from international norms and treaties in shaping the cybersecurity policies. This framework is also heavily based on countries that have existing strong cybersecurity structures and large budgets. This analysis acknowledges that while the framework is robust, its implementation must be adapted to specific political, cultural, and social contexts. From a public perspective it is dependent on the government to implement a framework like the proposed framework to ensure enough engagement to make their voices heard. Due to the structure of national governments the public is largely dependent on the structure coming from top down (Hassib and Shires, 2021). If the structure is not similar to the suggested policy the public should put pressure on governments to make changes. Future research should include a wider range of countries to include in the study. A good example is countries that are on the African continent. The countries that spark particular interest are the Democratic Republic of the Congo (DRC), South Africa, Egypt, Kenya, and Rwanda. These countries carry strong cyber policies but are vastly different on governmental structures (Hassib and Shires, 2021). Many others African countries have a strong diversity of political profiles that can be explored to improve the proposed framework. Researchers can further test and implement the proposed framework by mixing variables such as cultural attitudes toward cybersecurity, technological infrastructure capabilities, national security, and economic consequences. This framework might

be empirically investigated using real-world examples and case studies to get valuable insights into how applicable and flexible it is.

4. Conclusion

This systematic literature review investigated the complex relationship between political policymaking and public perceptions of cybersecurity. The study discovered that there are significant differences in how cybersecurity challenges are incorporated into policy frameworks. This was done by evaluating the perspectives from the selected countries. Despite this greater awareness the study also discovered a persistent gap in how these perceptions influence policy development. Many countries continuing to opt for reactive rather than proactive cybersecurity strategies. This led to the development of a cybersecurity framework. This framework ensures that the public have an equal but moderated say in policy creation. The framework also emphasises the importance of continual stakeholder engagement and fosters a symbiotic/holistic relationship between public concerns and government actions. The suggested framework intends to promote policies that are both comprehensive and resilient as well. The only probable issue is the small sample countries used. Further research would suggest a more complete methodology that includes a wider range of countries. For now, the framework is sufficed and can spark discussions on how the public can also have a voice in cyber policy creation.

References

Asllani, A. W., Charles Stephen Ettkin, Lawrence 2013. Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals. *J. Legal Ethical & Regul. Isses,* 16**,** 7.

Carr, M. & Lesniewska, F. 2020. Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance. *International Relations,* 34**,** 391-412.

Chowdhury, T. H., Parvez, N., Urmi, S. S. & Taher, K. A. Cybersecurity Challenges and Policy Options for Bangladesh. 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD), 27-28 Feb. 2021 2021. 472-476.

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J. & Weintrop, D. 2020. Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. *Simulation & Gaming,* 51**,** 586-611.

Dehghani, M., Niknam, T., Ghasemigarpachi, M., Alhelou, H. H., Pourbehzadi, M., Javidi, G. & Sheybani, E. 2023. Public policies for cyber security of sustainable dominated renewable smart grids. *IET Generation, Transmission & Distribution,* 17**,** 4057-4071.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. & Laplante, P. 2011. Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine,* 30**,** 28-38.

Hassib, B. & Shires, J. 2021. Manipulating uncertainty: Cybersecurity politics in Egypt. *Journal of Cybersecurity,* 7**,** tyaa026.

Kosseff, J. 2020. Hacking Cybersecurity Law. *U. Ill. L. Rev.,* 2020**,** 811.

Kshetri, N. 2020. The evolution of cyber-insurance industry and market: An institutional analysis. *Telecommunications Policy,* 44**,** 102007.

Li, Z. R., Guo, X. & He, Q. L. 2022. A Study of Chinese Policy Attention on Cybersecurity. *Ieee Transactions on Engineering Management,* 69**,** 3739-3756.

Manwaring, R., Holloway, J. 2023. Resilience to cyber-enabled foreign interference: citizen understanding and threat perceptions. *Defence Studies,* 23**,** 334-357.

Mugisha, D. 2019. *Methods and implementation to combat cyber crimes in Rwanda*. 10.13140/RG.2.2.20575.30888.

Nkongolo, M. 2023. Navigating the complex nexus: cybersecurity in political landscapes. *arXiv*.

Rupp, C., 2024. *Navigating the EU Cybersecurity Policy Ecosystem: A Comprehensive Overview of Legislation, Policies, and Actors*. Stiftung Neue Verantwortung (SNV).

Sivan-Sevilla, I. 2021. Framing and governing cyber risks: comparative analysis of U.S. Federal policies [1996–2018]. *Journal of Risk Research,* 24**,** 692-720.

Snider, K. L. G., Shandler, R., Zandani, S. & Canetti, D. 2021. Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity,* 7.

Subramanian, S. & Ward, M., 2022. *State Cybersecurity in a Heightened Risk Environment: 2022 Deloitte-NASCIO Cybersecurity Study*. Deloitte and the National Association of State Chief Information Officers (NASCIO).

Sutherland, E., 2017. *The National Cybersecurity Policy Framework (NCPF)*. In: *The African Journal of Information and Communication*, Issue 20, pp. 21-44.

Vilpišauskas, R. 2024. Gradually and then suddenly: the effects of Russia's attacks on the evolution of cybersecurity policy in Lithuania. *Policy Studies,* 45**,** 467-488.

Widjaja, G. 2023. Enhancing legal literacy: understanding the significance of law no. 9/2019 on electronic transactions in the social media era. *Journal of Community Dedication,* 3**,** 278-293.

Yusif, S., Hafeez-Baig, A. & Anachanser, C. 2024. Internet governance and cyber-security: a systematic literature review. *Information Security Journal: A Global Perspective,* 33**,** 158-171.