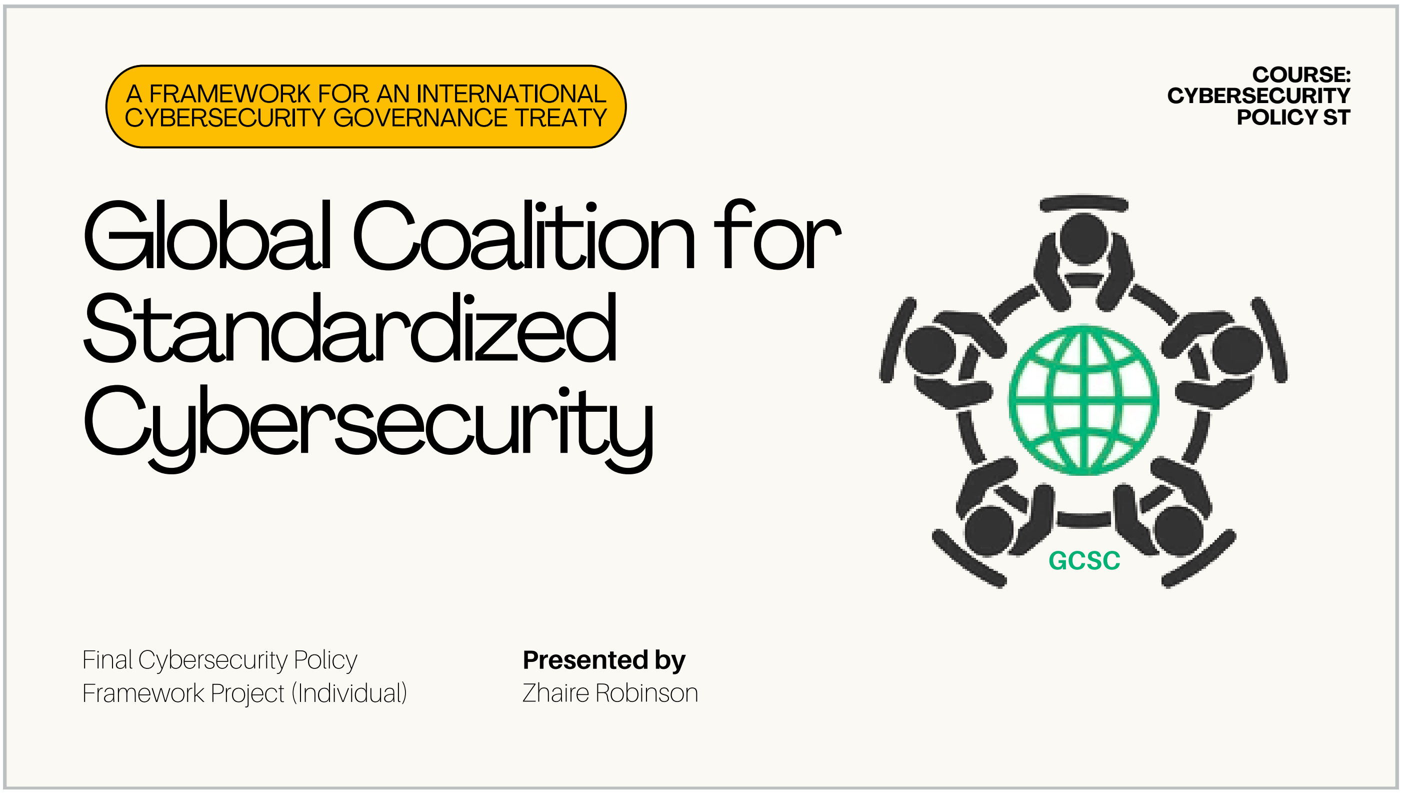


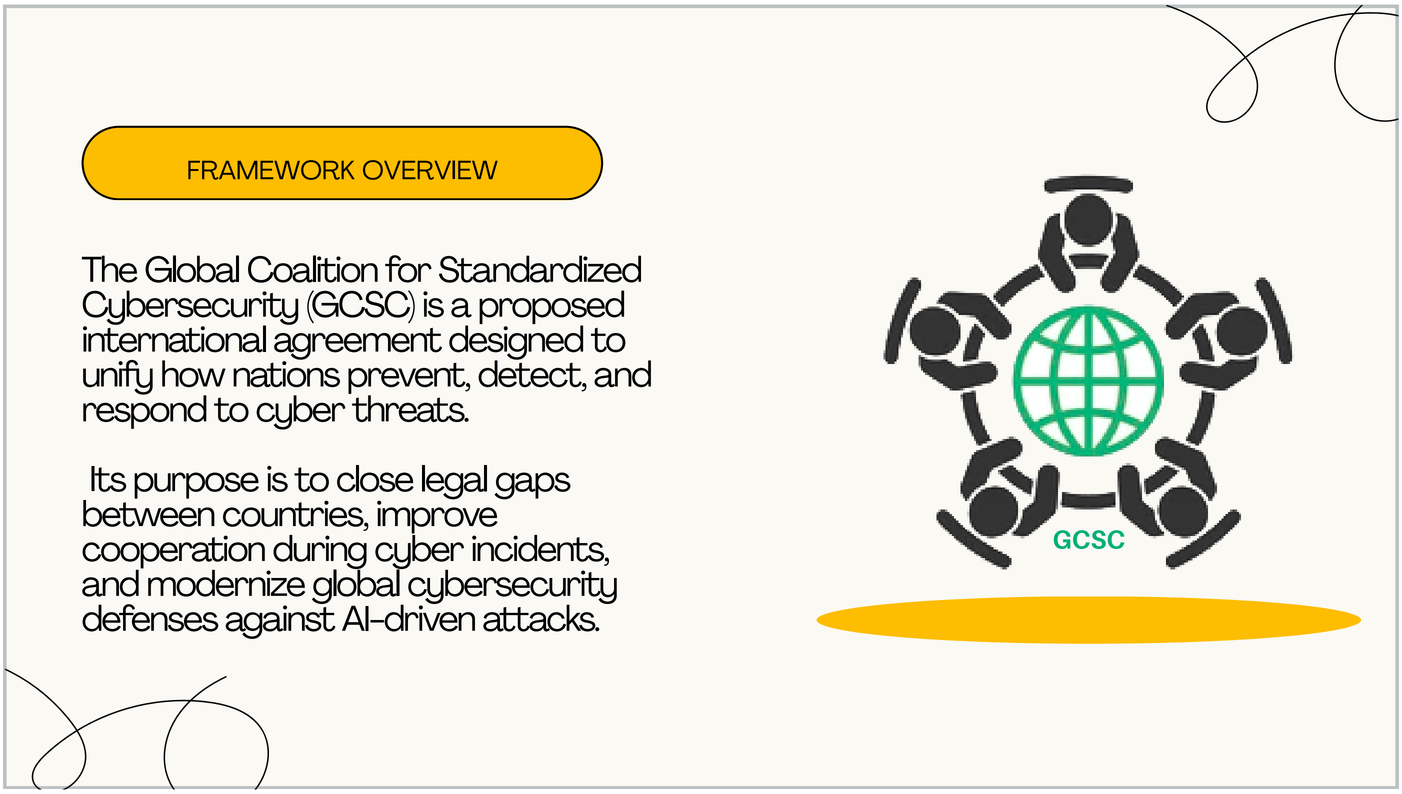
A FRAMEWORK FOR AN INTERNATIONAL CYBERSECURITY GOVERNANCE TREATY

COURSE:
CYBERSECURITY
POLICY ST

Global Coalition for Standardized Cybersecurity

Final Cybersecurity Policy Framework Project (Individual)

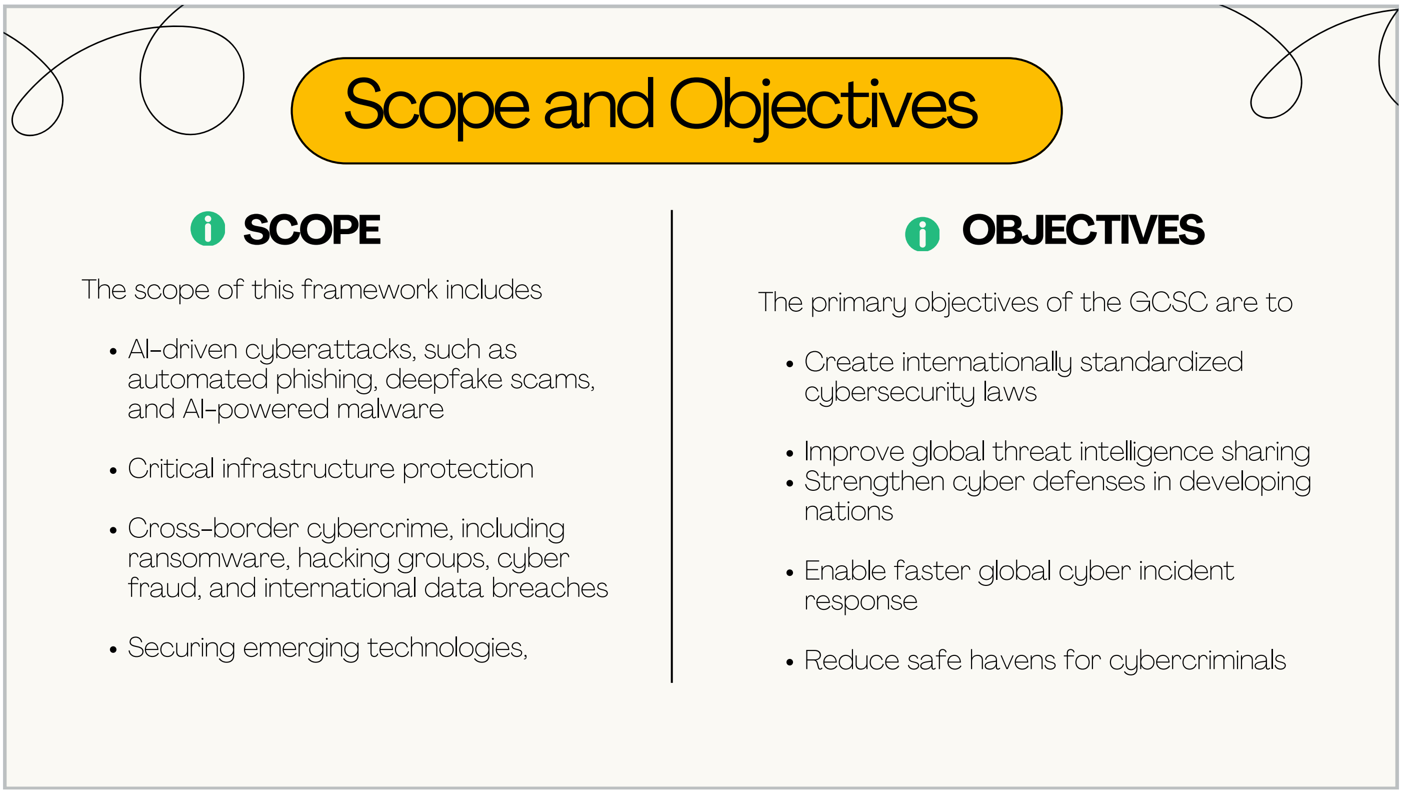
Presented by
Zhaire Robinson



FRAMEWORK OVERVIEW

The Global Coalition for Standardized Cybersecurity (GCSC) is a proposed international agreement designed to unify how nations prevent, detect, and respond to cyber threats.

Its purpose is to close legal gaps between countries, improve cooperation during cyber incidents, and modernize global cybersecurity defenses against AI-driven attacks.



Scope and Objectives

SCOPE

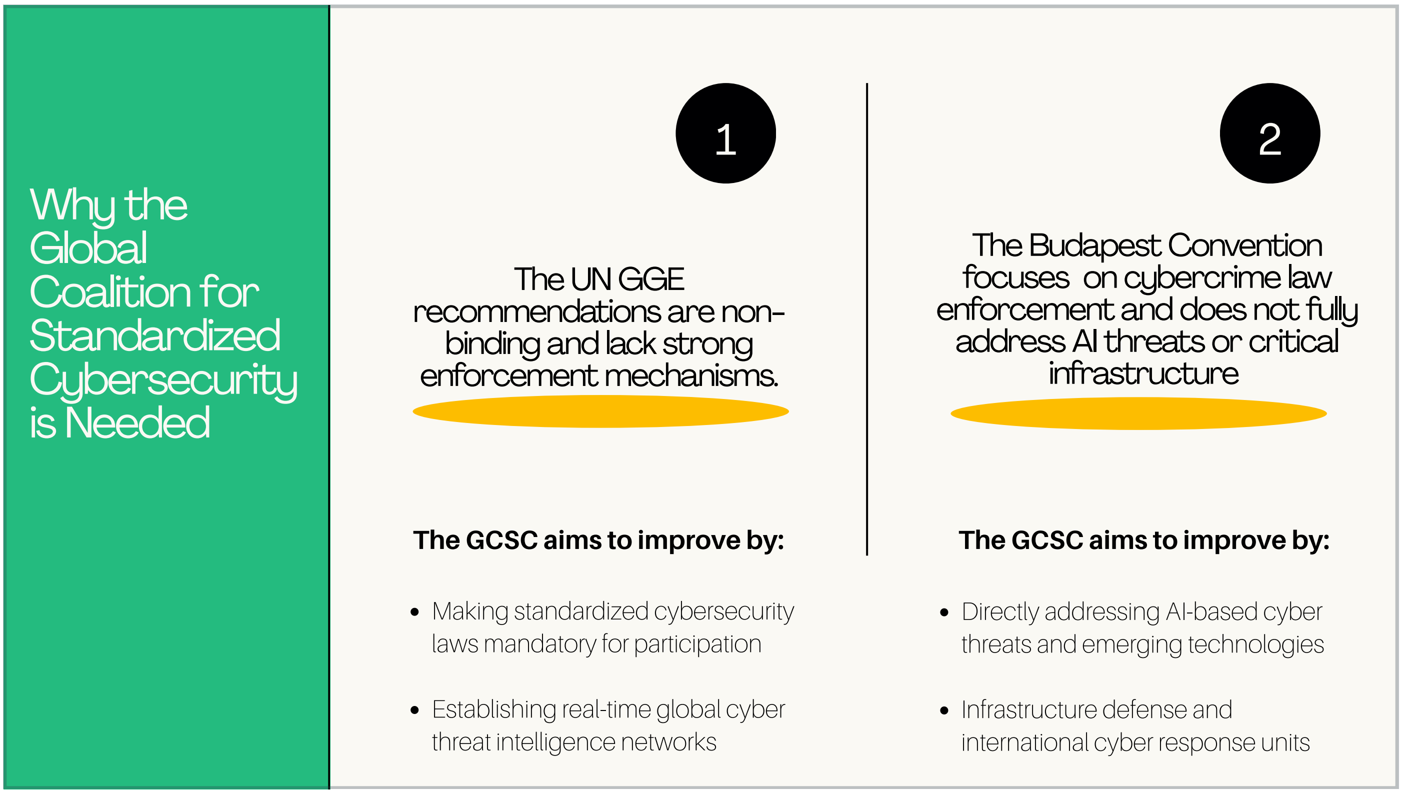
The scope of this framework includes

- AI-driven cyberattacks, such as automated phishing, deepfake scams, and AI-powered malware
- Critical infrastructure protection
- Cross-border cybercrime, including ransomware, hacking groups, cyber fraud, and international data breaches
- Securing emerging technologies,

OBJECTIVES

The primary objectives of the GCSC are to

- Create internationally standardized cybersecurity laws
- Improve global threat intelligence sharing
- Strengthen cyber defenses in developing nations
- Enable faster global cyber incident response
- Reduce safe havens for cybercriminals



Why the Global Coalition for Standardized Cybersecurity is Needed

1

The UN GGE recommendations are non-binding and lack strong enforcement mechanisms.

The GCSC aims to improve by:

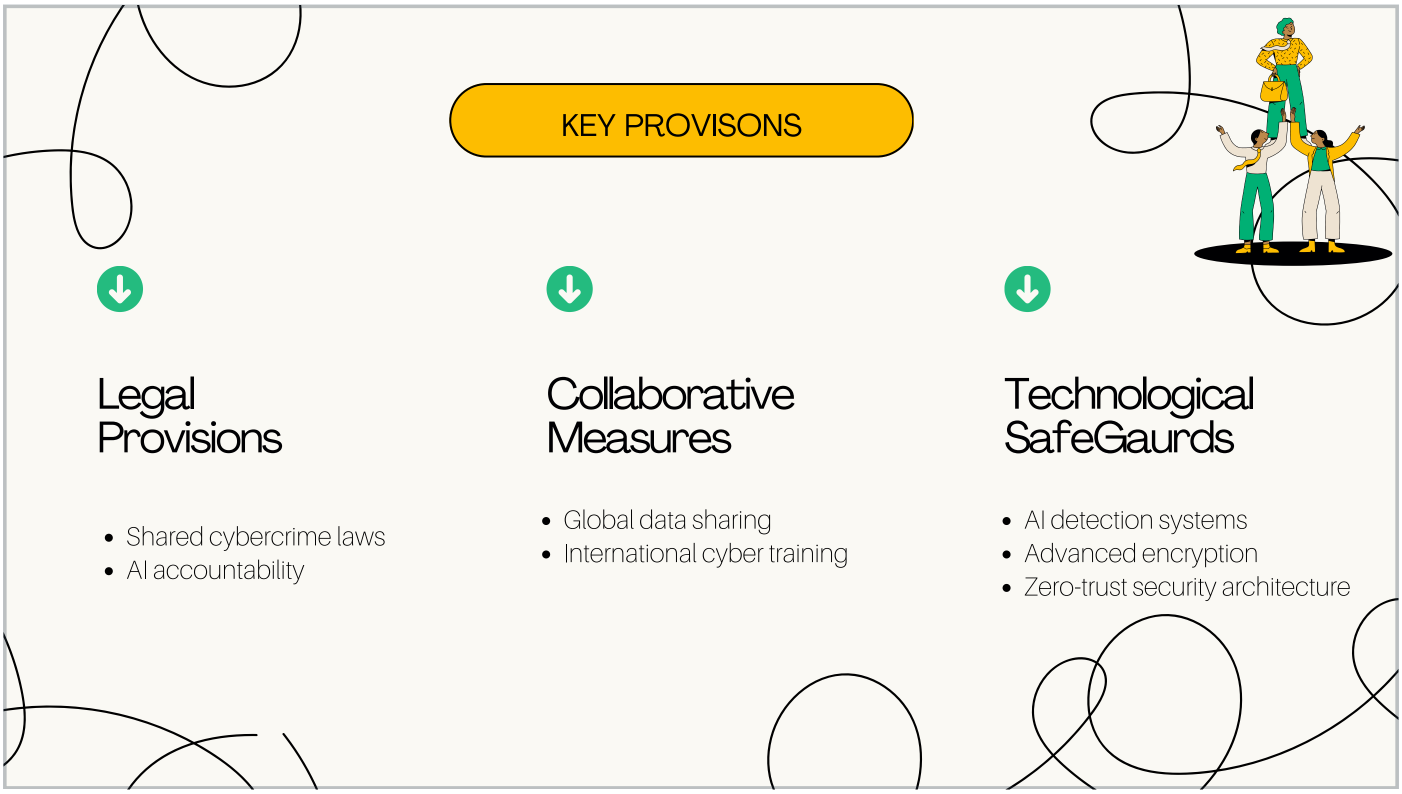
- Making standardized cybersecurity laws mandatory for participation
- Establishing real-time global cyber threat intelligence networks

2

The Budapest Convention focuses on cybercrime law enforcement and does not fully address AI threats or critical infrastructure

The GCSC aims to improve by:

- Directly addressing AI-based cyber threats and emerging technologies
- Infrastructure defense and international cyber response units



KEY PROVISONS

Legal Provisions

- Shared cybercrime laws
- AI accountability

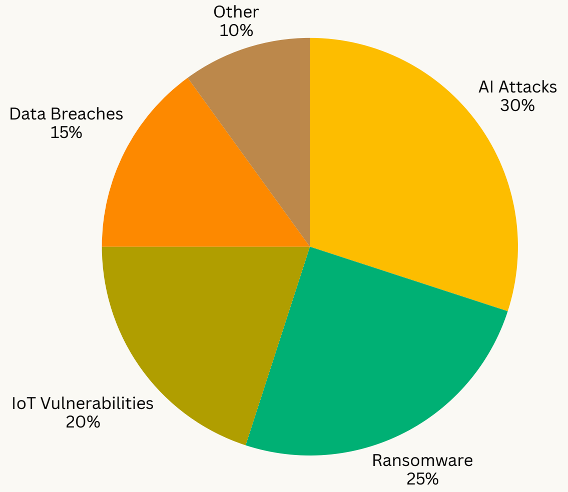
Collaborative Measures

- Global data sharing
- International cyber training

Technological SafeGaurds

- AI detection systems
- Advanced encryption
- Zero-trust security architecture

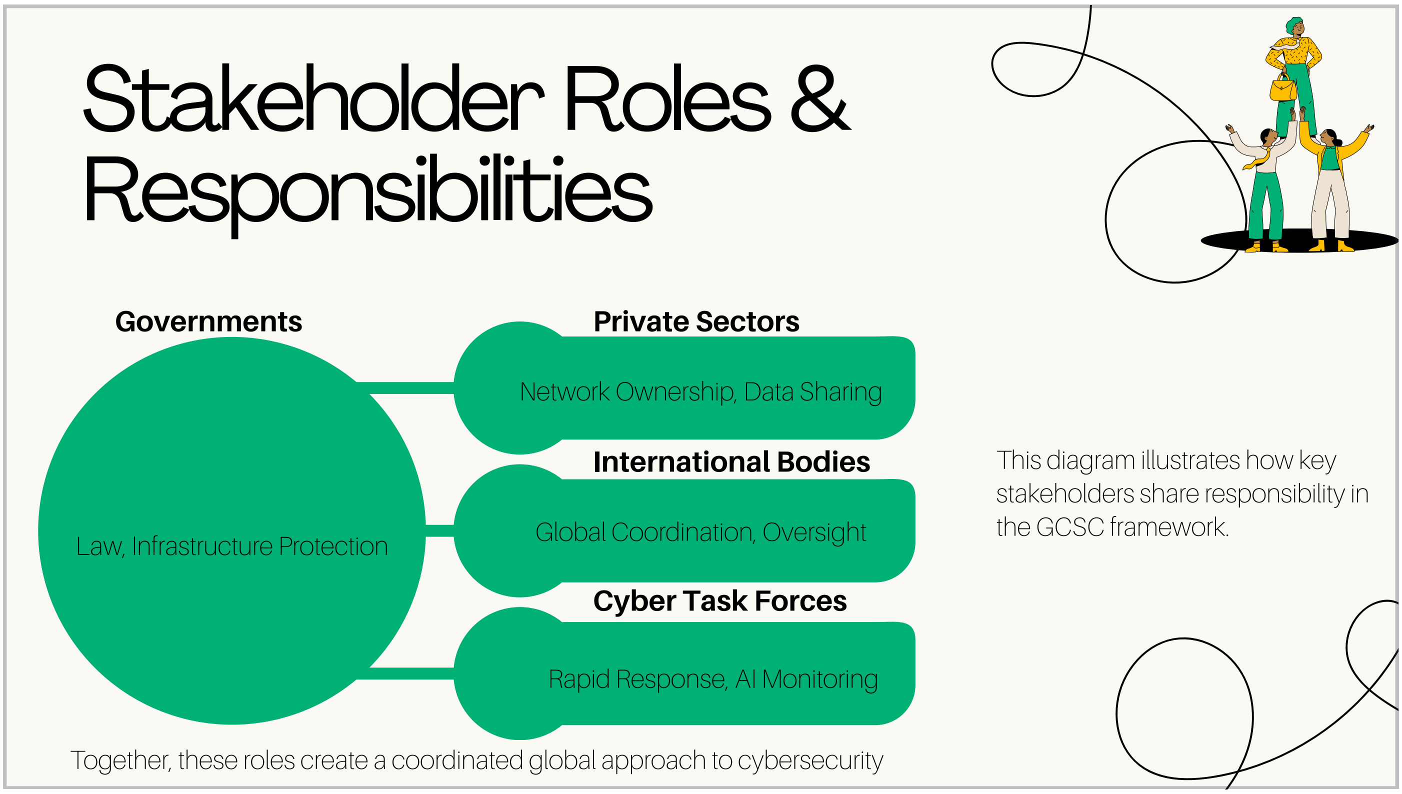
Legally, the framework establishes shared cybercrime laws and clear AI accountability to ensure consistent enforcement across nations. Collaboratively, it promotes global data sharing and international cybersecurity training programs to strengthen collective defense and knowledge exchange. Technologically, the coalition integrates AI-powered detection systems and advanced encryption to improve early threat detection and protect sensitive global communications.



Threat Scope Pie Chart
distribution of threats addressed by GCSC

These categories represent the highest-risk areas driving today's cyber threat landscape and justify the treaty's primary focus

This distribution is based on global cybersecurity reports showing ransomware as the most dominant threat, alongside the rapid rise of AI-driven attacks, IoT vulnerabilities, and large-scale data breaches.



Stakeholder Roles & Responsibilities

Governments

Law, Infrastructure Protection

Private Sectors

Network Ownership, Data Sharing

International Bodies

Global Coordination, Oversight

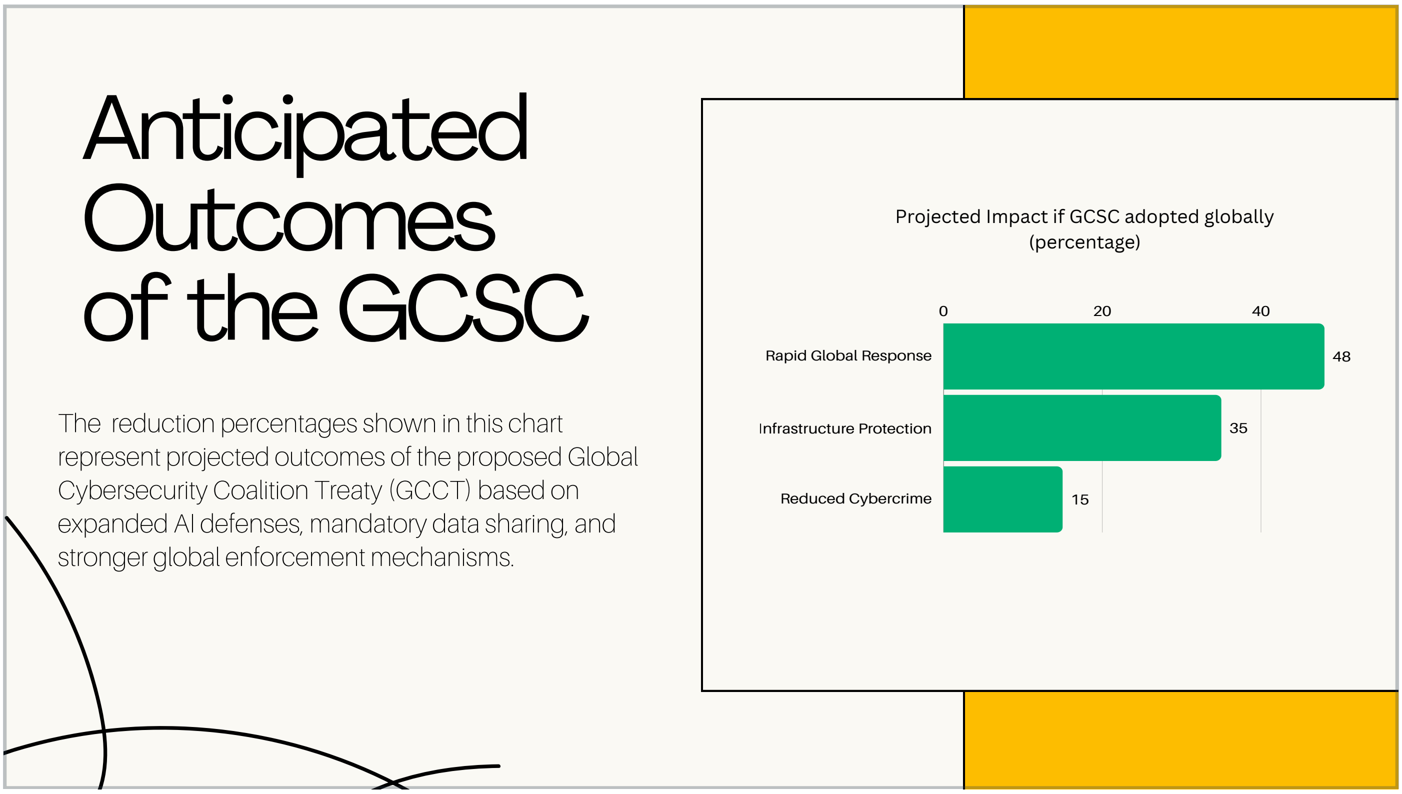
Cyber Task Forces

Rapid Response, AI Monitoring

This diagram illustrates how key stakeholders share responsibility in the GCSC framework.

Together, these roles create a coordinated global approach to cybersecurity

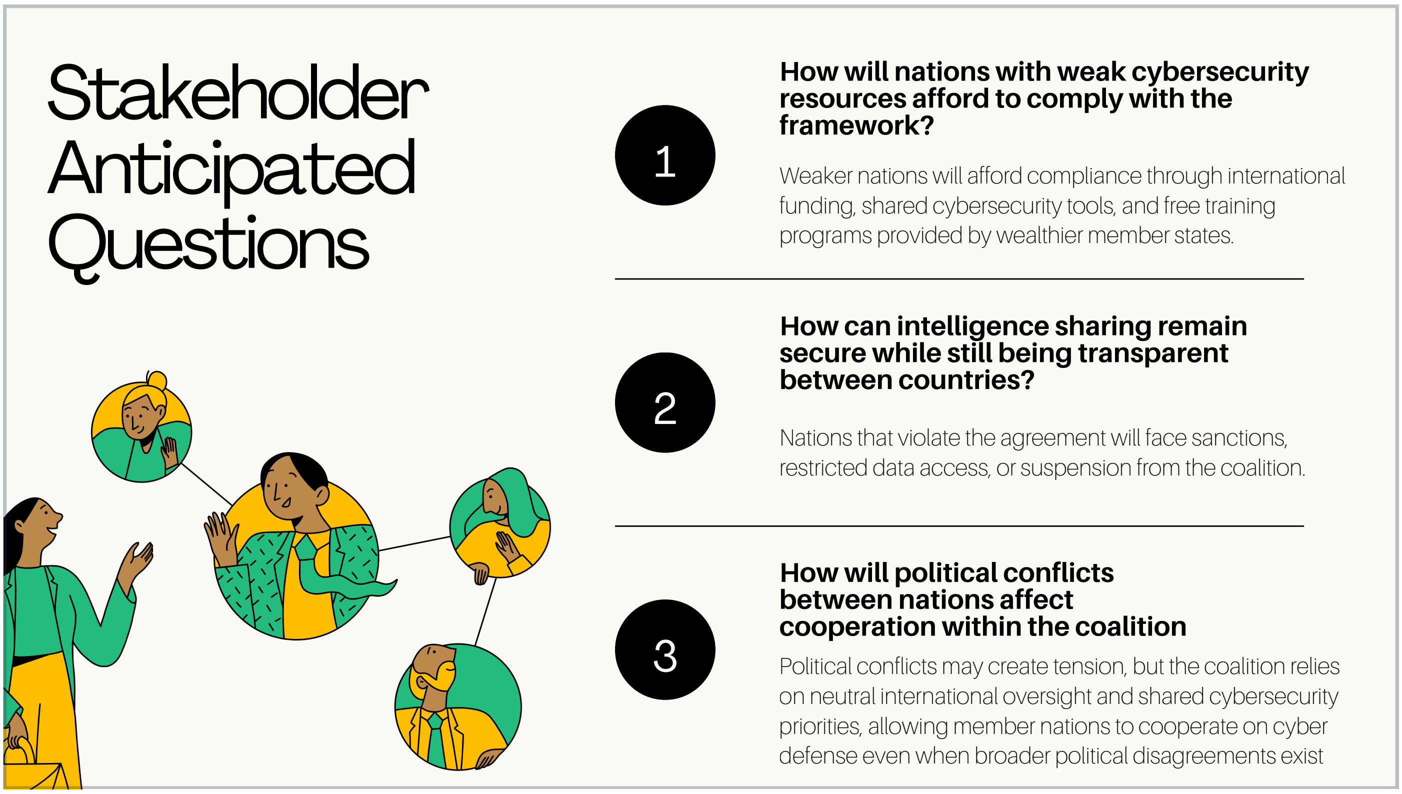
Governments handle law enforcement and protect critical infrastructure, the private sector manages networks and shares data, international bodies coordinate efforts across borders, and specialized cyber task forces provide rapid response to incidents



Anticipated Outcomes of the GCSC

The reduction percentages shown in this chart represent projected outcomes of the proposed Global Cybersecurity Coalition Treaty (GCCT) based on expanded AI defenses, mandatory data sharing, and stronger global enforcement mechanisms.

These are purely predictions loosely based off research and not full empirical evidence.



Stakeholder Anticipated Questions

1 **How will nations with weak cybersecurity resources afford to comply with the framework?**

Weaker nations will afford compliance through international funding, shared cybersecurity tools, and free training programs provided by wealthier member states.

2 **How can intelligence sharing remain secure while still being transparent between countries?**

Nations that violate the agreement will face sanctions, restricted data access, or suspension from the coalition.

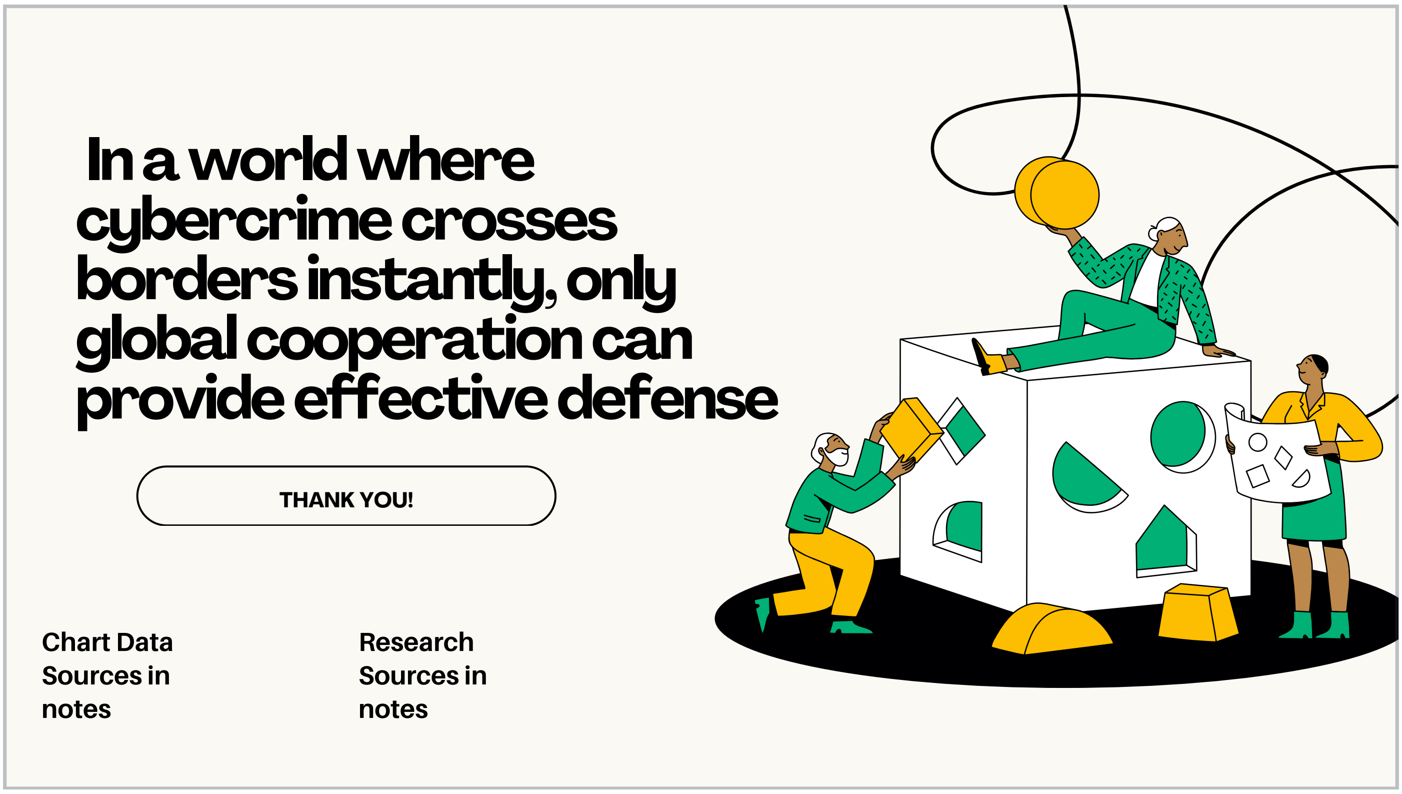
3 **How will political conflicts between nations affect cooperation within the coalition**

Political conflicts may create tension, but the coalition relies on neutral international oversight and shared cybersecurity priorities, allowing member nations to cooperate on cyber defense even when broader political disagreements exist

CONCLUSION

The Global Coalition for Standardized Cybersecurity (GCSC) provides a modern solution to modern cyber threats.

By unifying international cybersecurity laws, improving cooperation, and integrating advanced technologies, this framework strengthens global digital security.



In a world where cybercrime crosses borders instantly, only global cooperation can provide effective defense

THANK YOU!

Chart Data Sources in notes

Research Sources in notes

Other Sources:

Picture: 472,888 global connections icon stock vectors and vector art | shutterstock. (n.d.). https://www.shutterstock.com/search/global-connections-icon?image_type=vector&dd_referrer=

Research Sources:

Ariel Tseitlin, S. S. (2025, April 24). 2025 state of Cybersecurity. Scale Venture Partners. https://www.scalevp.com/insights/2025-state-of-cybersecurity/

Global State of Cybercrime Legislation 2013-2023. (n.d.-b). https://rm.coe.int/3148-1-3-4-cyberleg-global-state-dec-2023-v4-public/1680adadf0

3.7 cybercrime. Eurojust. (n.d.). https://www.eurojust.europa.eu/annual-report-2023/cybercrime

Chart Data Sources:

Cybercrime statistics: Key stats and insights. Verimatrix. (2025, June 11). https://www.verimatrix.c om/cybersecurity/knowledge-base/cybercrime-statistics-key-stats-and-insights/

Keepnet Labs. (n.d.). 300 cyber security statistics, facts, figures (nov 2025) - keepnet. https://keep netlabs.com/blog/cyber-security-statistics-and-trends?

Cybersecurity Trends & Predictions 2025 CERT-Mu april 2025. (n.d.-b). https://cert-mu.govmu.org/ cert-mu/wp-content/uploads/2025/04/Cybersecurity-Trends-and-Predictions-2025.pdf

Fox, J. (2025, November 19). Top cybersecurity statistics for 2025. Pentest as a Service. https://www.cobalt.io/blog/top-cybersecurity-statistics-2025