Chaudhary, A. (2025). Proposal for a Global Cybersecurity Alliance. *Journal for Global Business and Community*, *16*(1), 1–4. https://doi.org/10.56020/001c.134053

Essays

Proposal for a Global Cybersecurity Alliance

Ayushi Chaudhary[1]

[1] Temple University

Keywords: cybersecurity, cyberattacks, national security, intelligence sharing, digital threats

https://doi.org/10.56020/001c.134053

Journal for Global Business and Community

Vol. 16, Issue 1, 2025

Cyberattacks are among the most critical threats facing the U.S. and the global community, with the potential to disrupt national security, critical infrastructure, and the global economy. In 2024, the cost of cyberattacks was estimated at $9.5 trillion, highlighting the urgency for a collective response. This proposal advocates for the creation of a Global Cybersecurity Alliance (GCA), led by the United States, to address the evolving cybersecurity challenge through multinational cooperation. The GCA will focus on four key areas: cross-border intelligence sharing, cybersecurity standardization, workforce development, and critical infrastructure protection. The alliance will unite nations—including the U.S., European Union, Indo-Pacific countries, and developing nations—under a unified defense strategy to safeguard global digital infrastructure and ensure long-term security and stability. This initiative aims to enhance international cybersecurity efforts, strengthen global resilience against cyber threats, and promote a secure digital future for all nations.

Dear Mr. President:

The growing threat of cyberattacks is one of the most pressing issues facing the incoming U.S. administration. With the potential to disrupt national security, cripple critical infrastructure, and damage the global economy, cyber threats pose a grave risk that requires immediate action. In 2024 alone, the global cost of cyberattacks was $9.5 trillion, with the U.S. being among the hardest-hit nations. These attacks have evolved in sophistication, and the involvement of both state and non-state actors has made cybersecurity an issue that transcends national borders. The interconnected nature of the digital world means no nation can effectively defend against these threats alone.

To address this challenge, I propose the establishment of a Global Cybersecurity Alliance (GCA), a coordinated, multinational initiative led by the United States. The GCA will bring together key global stakeholders—including the European Union (EU), Indo-Pacific nations, and developing countries—to forge a collective defense strategy against cyber threats. The alliance will focus on four key areas:

- Cross-Border Intelligence Sharing
- Cybersecurity Standardization
- Workforce Development
- Critical Infrastructure Protection

By establishing the GCA, the United States will lead the way in creating a unified global defense against cyberattacks, ensuring not only national security but also global stability in the current age of information.

The Growing Cybersecurity Threat

The digital era has fundamentally transformed modern life, revolutionizing communication, trade, governance, and defense. However, it has also introduced new vulnerabilities that cybercriminals and state-sponsored actors are eager to exploit. As both the global economy and military operations increasingly rely on digital systems, the risks associated with cyberattacks have escalated dramatically. In 2024, cyberattacks inflicted global economic damage estimated at $9.5 trillion, with industries such as healthcare, finance, energy, and defense being left particularly vulnerable.

Cyber threats have evolved from isolated, low-level attacks to large-scale, sophisticated campaigns targeting government systems, stealing intellectual property, and disrupting critical infrastructures. One of the most notorious examples is the 2020 SolarWinds breach, attributed to Russian hackers, which compromised U.S. government agencies and private corporations. This breach demonstrated how easily trusted systems can be infiltrated, putting national security and economic stability at risk. Similarly, the rise of ransomware attacks on U.S. hospitals in 2024 highlighted how cyberattacks can disrupt vital public services, jeopardizing lives and the delivery of essential care.

These cyberattacks are increasingly perpetrated by state-sponsored actors, including China, Russia, and North Korea, who employ cyber tools for espionage, military advantage, and economic disruption. These threats are not limited to military or defense systems; they extend to private industries, critical infrastructure, and global supply chains. For instance, a cyberattack on Japan's defense sys-

tems could disrupt U.S. military operations in the Indo-Pacific, destabilizing the region and impacting the balance of global power. Similarly, an attack on European financial institutions could reverberate throughout global markets, impacting the global economy.

The transnational nature of these cyber threats means that the actions of one nation can have far-reaching consequences for others. A successful cyberattack on one country can have cascading effects that destabilize entire industries, regions, and even global security frameworks. As such, cybersecurity is no longer a solely national concern but a global one, requiring international cooperation and leadership.

The Plan: Establishing the Global Cybersecurity Alliance (GCA)

The proposed Global Cybersecurity Alliance (GCA) is a bold, proactive initiative that will unite the United States, its allies, and other global stakeholders in a collective effort to combat cyber threats. The GCA will focus on four primary initiatives: Cross-Border Intelligence Sharing, Cybersecurity Standardization, Workforce Development, and Critical Infrastructure Protection. These initiatives will lay the groundwork for a unified international strategy to counter evolving cyber threats.

Cross-Border Intelligence Sharing

A major challenge in modern cybersecurity is the lack of real-time, actionable intelligence. Cyberattacks are often carried out by actors across multiple borders, making it difficult for individual nations to track, respond to, and prevent these attacks on their own. As cybercriminals and state-sponsored hackers evolve, their attacks grow faster and become increasingly difficult to detect. This necessitates coordinated efforts to address emerging threats.

The GCA will establish secure, real-time platforms for intelligence sharing across member countries. These platforms will facilitate the exchange of crucial information regarding emerging threats, vulnerabilities, malware, and attack techniques. By sharing intelligence in real-time, countries can respond more swiftly and effectively to potential cyberattacks. The creation of a Global Cyber Threat Intelligence Network, modeled after successful initiatives such as the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), will facilitate the exchange of data on attack patterns, intrusion attempts, and countermeasures. This approach has already proven effective in smaller-scale collaborations and can be expanded globally to safeguard member nations.

Cybersecurity Standardization

The disparity in cybersecurity standards across nations is a significant vulnerability. Countries operate under different legal frameworks and policies, and cybersecurity preparedness varies widely. This inconsistency creates gaps that can be exploited by cybercriminals and state-sponsored hackers, particularly when targeting nations with weaker defenses. It also complicates global coordination in responding to cyberattacks.

The GCA will work to standardize cybersecurity protocols across member nations, establishing global best practices for securing data, implementing encryption, and responding to cyber incidents. By aligning cybersecurity standards, the GCA will make it more difficult for attackers to find weaknesses in the global digital infrastructure. Additionally, standardization will make it easier for countries to cooperate and coordinate responses to large-scale cyberattacks, ensuring a unified defense against common threats.

One of the GCA's key goals will be to bridge the cybersecurity gap between developed and developing nations. Many developing nations lack the resources to implement strong cybersecurity measures, leaving them vulnerable to exploitation. The GCA will provide these nations with the tools, knowledge, and resources needed to adopt international best practices, ensuring that all members, regardless of economic standing, are adequately protected against cyber threats.

Workforce Development

A significant challenge facing the global cybersecurity community is the shortage of skilled professionals. The Cybersecurity and Infrastructure Security Agency (CISA) reports a global shortage of over 3 million cybersecurity professionals, a gap that leaves nations vulnerable to attacks. Addressing this shortage will require a coordinated effort to build a robust global cybersecurity workforce capable of responding to increasingly complex cyber threats.

The GCA will focus on workforce development through education, training, and capacity-building initiatives. By establishing joint educational programs, creating cybersecurity training hubs, and offering scholarships, the GCA will ensure that countries around the world are equipped with the talent needed to tackle cybersecurity challenges. Special emphasis will be placed on developing countries, where local talent is often underutilized due to a lack of resources. These initiatives will not only strengthen the cybersecurity capabilities of member nations but also create a sustainable workforce that can adapt to future challenges.

Critical Infrastructure Protection

Critical infrastructure, including energy grids, healthcare systems, transportation networks, and financial institutions, is a primary target for cyberattacks. Attacks on these systems can have devastating consequences, disrupting essential services and causing widespread damage. The GCA will prioritize protecting critical infrastructure through various initiatives, including joint cybersecurity exercises, the promotion of cybersecurity best practices, and the establishment of guidelines for securing vital sectors.

By collaborating on the identification and mitigation of vulnerabilities in critical infrastructure, GCA members will be better prepared to respond to cyberattacks when they occur. Regular cybersecurity drills and simulating large-

scale attacks on critical sectors will allow countries to practice coordinated responses and strengthen their ability to recover quickly from cyber incidents. These exercises will help ensure that, should an attack occur, member nations can minimize its impact and restore essential services as quickly as possible.

Regional and Global Cooperation

Indo-Pacific Region

The Indo-Pacific region represents one of the most dynamic and rapidly evolving digital economies in the world, yet it remains highly vulnerable to cyberattacks. Geopolitical tensions, especially with China and North Korea, further heighten the risks faced by nations in this region. Countries including Japan, South Korea, India, and Australia have made strides in improving their cybersecurity defenses but still face significant challenges, particularly in protecting critical infrastructure sectors like defense, energy, and finance.

The U.S. has a direct interest in ensuring the cybersecurity of its Indo-Pacific allies. For instance, Japan hosts over 54,000 U.S. military personnel, the largest concentration of American forces outside the United States. A successful cyberattack on Japan's defense systems could destabilize U.S. military operations in the region, compromising overall security in the Indo-Pacific. Similarly, North Korea's repeated targeting of South Korea's military and financial sectors highlights how cyber threats in the region can directly affect U.S. national security interests. The GCA will work closely with Indo-Pacific nations to enhance their cybersecurity capabilities, ensuring that the region is better protected against evolving threats.

European Union (EU)

The European Union has long been a leader in cybersecurity, setting standards that have been adopted worldwide. Policies like the General Data Protection Regulation (GDPR) have revolutionized the way that nations handle data privacy and security. The EU's ability to coordinate cybersecurity efforts among its member states will be invaluable to the success of the GCA. By including the EU in the alliance, the U.S. can ensure that Europe's cybersecurity measures are integrated into a global framework.

A cyberattack on European infrastructure could have devastating consequences for both European nations and the global economy. The close economic ties between the U.S. and the EU make it essential that their cybersecurity efforts are aligned. By incorporating the EU into the GCA, the U.S. will strengthen its own cybersecurity defenses while contributing to global stability.

Developing Countries

The GCA will also focus on building the cybersecurity capacity of developing nations, which are often the most vulnerable to cyber threats. Many countries in Africa, Latin America, and Southeast Asia lack the resources and expertise to protect themselves against cyberattacks. By partnering with these nations, the GCA will help close the digital divide and ensure that all countries, regardless of economic status, can defend themselves against cyber threats.

Inclusion of developing nations in the GCA will promote a more comprehensive and resilient global cybersecurity network, where every member has the tools and knowledge necessary to protect themselves and contribute to collective defense against cyberattacks.

Impact on U.S. National Security

The creation of the Global Cybersecurity Alliance (GCA) would have profound implications for U.S. national security. As cyberattacks increasingly target critical U.S. infrastructure, such as defense systems, energy grids, and financial institutions, a collective defense framework would bolster the nation's ability to mitigate these threats. The impact of a successful cyberattack on the U.S. could be devastating, potentially leading to a loss of military advantage, significant economic disruptions, and damage to national infrastructure. By leading the charge in establishing the GCA, the U.S. would be strengthening its own defenses while fortifying those of its global allies.

Protection of Critical Infrastructure

Cyberattacks targeting U.S. infrastructure can cripple essential services, leading to long-term national security consequences. A breach in energy grids, transportation systems, or healthcare networks could severely impair the country's ability to operate effectively. With the GCA in place, the U.S. can work with its international partners to establish shared security protocols for safeguarding critical infrastructure. By ensuring that global partners adopt the same cybersecurity standards, the GCA reduces vulnerabilities across borders, which, in turn, strengthens the security of U.S. systems and military operations.

Deterrence of Adversaries

A unified global approach to cybersecurity would send a clear message to adversaries that cyberattacks against the United States and its allies will not go unchallenged. With a network of countries committed to collaborative defense, the GCA would create a strong deterrent against cyber-espionage, theft, and attacks by state-sponsored hackers. As adversaries such as China, Russia, and North Korea continue to pose cyber threats to U.S. interests, the GCA presents a united front that makes it more difficult for these actors to exploit weaknesses in individual countries' defenses.

Enhanced Military Operations

In today's digital era, modern warfare increasingly relies on secure communication and data-sharing platforms. Cyberattacks targeting U.S. military networks could disrupt command and control systems, leading to a potential loss of operational effectiveness. By integrating global cybersecurity efforts, the U.S. can enhance the resilience of its

military infrastructure and ensure that its defense systems are secure from external interference. Additionally, promoting closer cybersecurity cooperation with allies in regions such as the Indo-Pacific is essential to maintaining military readiness and ensuring the security of U.S. military operations abroad.

Cybersecurity of U.S. Allies

U.S. national security is intrinsically linked to the security of its allies, particularly in critical regions such as Europe and the Indo-Pacific. A cyberattack on an ally's infrastructure could have far-reaching consequences for U.S. military, economic, and political interests. For instance, a cyberattack on Japan's defense systems, as a key U.S. ally, could disrupt U.S. military operations in the Indo-Pacific, impacting both regional security and broader U.S. defense strategies. By leading the creation of the GCA, the United States ensures that its allies are better prepared to withstand cyberattacks, contributing to global stability and safeguarding American interests in the process.

Strengthening Global Supply Chains

The interconnectedness of global supply chains means that a cyberattack on key sectors, whether in the energy, manufacturing, or financial industries, can quickly escalate to impact the U.S. economy. By promoting stronger cybersecurity protocols across nations, the GCA will help secure the global digital supply chain, reducing the risk of disruptions that could directly affect U.S. businesses. For instance, cyberattacks targeting European financial institutions or Asian tech companies could have ripple effects on U.S. markets. Strengthening cybersecurity internationally mitigates the risks to U.S. economic stability and protects the nation's global interests.

Expanding U.S. Cybersecurity Capabilities

As the U.S. works with international partners through the GCA, it gains access to innovative technologies, intelligence, and cybersecurity innovations. Sharing information on emerging threats and best practices will help the U.S. stay at the forefront of cybersecurity advancements, enhancing its own national capabilities. By building a robust network of cybersecurity professionals globally, the U.S. can tap into international expertise to respond more effectively to emerging threats. This global collaboration ensures that the U.S. not only contributes to international cybersecurity efforts but also strengthens its own national security infrastructure.

Conclusion

Cybersecurity is no longer a matter of individual national interest but a global challenge that requires collective action. The establishment of the Global Cybersecurity Alliance will provide a platform for nations to work together to combat cyber threats, protect critical infrastructure, and ensure the stability of the global digital economy. By leading this effort, the United States can strengthen its own security while enhancing global resilience against cyberattacks. The time to act is now. Through the GCA, the U.S. can lead the world in building a secure, stable, and resilient digital future.

Submitted: February 14, 2025 EDT. Accepted: February 21, 2025 EDT. Published: April 07, 2025 EDT.