Expanding the Cyber Mission Space with the Expansion of Security Cooperation in the Era of Great Power Competition

Ariel Rosario, Timothy Shives and Mustafa Canan
Naval Postgraduate School, USA

ariel.rosario@nps.edu
timothy.shives@nps.edu
anthony.canan@nps.edu

Abstract: As great power competition intensifies, cybersecurity has emerged as both a battleground and an opportunity for cooperation. Malign actors exploit cyber infrastructure to undermine international order while simultaneously presenting themselves as contributors to economic growth. This paper proposes a novel framework for managing cybersecurity challenges by establishing regional Cyber Centers of Excellence (CCoEs), aligned with existing internet governance structures. The research outlines three key contributions: (1) mapping cyberspace governance to align cyber defense responsibilities with existing regional partnerships, (2) enhancing multinational mission assurance through CCoEs as collaborative hubs, and (3) leveraging proactive cyber operations such as "hunt forward" to increase partner capacity against cyber threats. By integrating established security cooperation mechanisms with new cybersecurity frameworks, this paper offers policymakers and cybersecurity professionals a roadmap to strengthen global cyber defense efforts while balancing national sovereignty and collective security.

Keywords: Cyberspace expansion, Security cooperation, Defend/hunt forward, Cyber alliances

1. Introduction

The cybersecurity landscape is rapidly evolving, driven by geopolitical competition and the strategic importance of digital infrastructure. As nations vie for cyber dominance, cooperation remains essential to managing collective threats. However, ambiguous governance frameworks and diverging state interests complicate international collaboration.

The transition from the Internet Assigned Numbers Authority (IANA) to the Internet Corporation for Assigned Names and Numbers (ICANN) symbolized a shift toward a multi-stakeholder model of internet governance (Hill, 2016). However, the decentralized model has also intensified geopolitical tensions, particularly between the United States and China. China's doctrine of "cyber sovereignty" contrasts sharply with Western ideals of an open and decentralized internet (Hoffmann et al., 2020), leading to fragmentation and competing visions of cyberspace governance.

This paper introduces a framework that reconciles national sovereignty with collective cybersecurity, leveraging regional partnerships to align cyber defense responsibilities. It proposes a geopolitical framework for cyber boundary management that aligns with existing internet governance structures, specifically the Regional Internet Registry (RIR) system. This paper introduces the concept of Cyber Centers of Excellence (CCoEs) as a mechanism for enhancing mission assurance in multinational operational cyberspace. It evaluates the potential of "hunt forward" operations and other low-cost mechanisms to increase partner capacity against malicious cyber activities. It offers a comprehensive model for building trust and sharing intelligence among allies in cyberspace, drawing inspiration from existing frameworks like the Five Eyes alliance.

1.1 Geopolitical Context of Cybersecurity

China's approach to internet governance is rooted in its concept of "cyber sovereignty," which asserts the right of states to regulate and control their cyberspace (Creemers, 2020). This model has several key components such as: China's "Great Firewall", a sophisticated system of internet censorship and surveillance, which restricts access to foreign websites and monitors domestic internet traffic (King et al., 2013). Data localization laws which are regulations requiring foreign companies to store Chinese users' data within China's borders, as exemplified by the 2017 Cybersecurity Law (Sacks, 2018). Indigenous innovation policies promoting the development of domestic technology to reduce reliance on foreign IT systems (Lindsay, 2015). In 2020, China launched its Global Initiative on data security, proposing a set of international rules for data governance that emphasizes state sovereignty over data flows (Ministry of Foreign Affairs of the People's Republic of China, 2020).

In contrast, the United States advocates for a multi-stakeholder model of internet governance by emphasizing open, free flow of information across the Internet, the encouragement of private sector leadership and self-regulation, and fostering alliances and partnerships for collective security. For example, the Clean Network

initiative, launched in 2020, aimed to create a coalition of "trusted" countries and companies to exclude Chinese technology from critical infrastructure (U.S. Department of State, 2020).

1.2 Implications for Global Cybersecurity

The divergence between these approaches has significant implications for global cybersecurity efforts. The fragmentation of cyberspace threatens the emergence of separate “internets” governed by different rules and practices. This division complicates international cooperation, as differing views on data privacy, content regulation, and cyber operations hinder the establishment of global cybersecurity norms (Kello, 2017). Additionally, supply chain security remains a critical concern, with fears over hardware and software vulnerabilities prompting restrictions on technology imports, such as the U.S. actions against Huawei (Lysne, 2018). Heightened tensions over cyber espionage and intellectual property theft further exacerbate geopolitical struggles, as seen in the 2015 U.S.-China agreement on commercial cyber espionage (Harold et al., 2016). Meanwhile, digital trade barriers arising from conflicting regulations on data localization and cross-border data flows create significant obstacles for global digital commerce (Aaronson & Leblond, 2018). Understanding this geopolitical context is crucial for developing effective international cybersecurity frameworks, as the proposed CCoEs must navigate these competing visions of cyber governance while fostering cooperation on shared security challenges.

2. Cyberspace Boundary Management

Cyber boundaries are inherently ambiguous, lacking the clear jurisdictional demarcations of physical domains. This ambiguity complicates attribution, erodes trust, and weakens collective cybersecurity efforts. In response, this paper proposes mapping cyberspace governance according to geopolitical boundaries, using the existing Regional Internet Registry (RIR) system as a model.

The RIR (2022) governance model integrates three critical factors: community policy, national legal frameworks, and technical remit. Similarly, CCoEs can establish community-driven policies that define roles, responsibilities, and information-sharing protocols, ensuring participants adhere to standardized cybersecurity operations. Aligning with national legal frameworks, CCoEs can clarify jurisdictional boundaries, ensure compliance with domestic and international laws, and prevent regulatory overlaps, fostering transparent and effective governance.

CCoEs would also provide technical coordination and expertise by monitoring cyber threats, facilitating information-sharing, and offering specialized training. This structure enhances operational effectiveness and minimizes ambiguity in cyber incident responses. By integrating policy, legal, and technical domains, CCoEs can function as trusted intermediaries, strengthening collaborative governance and improving international cybersecurity coordination.

This framework balances national sovereignty, international cooperation, and cybersecurity standards by aligning CCoE jurisdictions with the five RIRs. Each region would define a “cyber territory” encompassing: government networks and systems, critical infrastructure (e.g., power grids, water systems), private-sector networks registered within national borders, and citizen data stored on domestic servers.

Regional CCoEs would exercise full sovereignty over these domains, with jurisdictional oversight over cyber activities within their physical boundaries. This model mirrors the RIRs’ success in managing global internet resources while promoting transparency and accountability.

2.1 Cyberspace Mapping Initiative

RIRs manage the allocation, administration, and registration of Internet number resources, including IPv4/IPv6 addresses and Autonomous System Numbers (ASNs). Operating under a multi-stakeholder model, RIRs facilitate policy development and technical coordination to ensure internet stability (RIR System, 2022).

The five RIRs govern IP allocations based on geographical regions, as shown in Figure 1: North American oversight is provided by the ARIN. In Europe, the Middle East, and Central Asia the RIPE NCC facilitates RIR services, Asia-Pacific region is provided by the APNIC, Latin America and Caribbean regions are managed by the LACNIC and across the African continent the AFRINIC manages services.

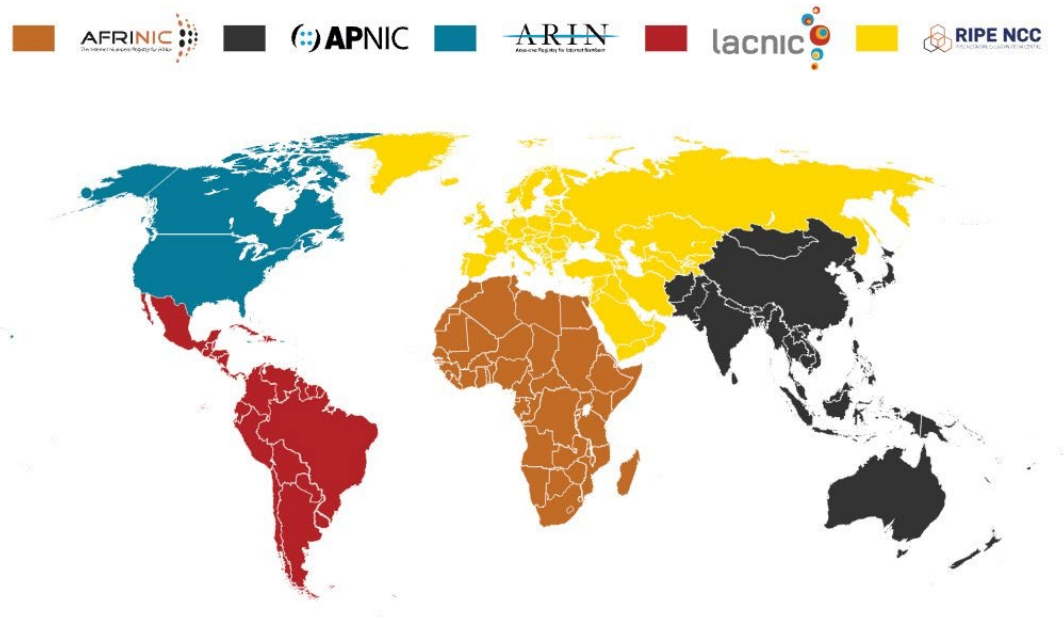

Figure 1: RIR Geographic Coverage

Note. Figure derived from ICANN ASO. (2022). *RIR governance model*.

Regional cooperation in cyberspace governance can leverage existing geopolitical collaborations. For instance, South American nations such as Brazil, Chile, and Argentina already cooperate on economic and security initiatives. Expanding these frameworks to cyber governance under LACNIC would enhance transparency and trust, ensuring nations take responsibility for specific cyber sectors.

The RIR governance model supports a bottom-up policy development approach, fostering trust and inclusivity among stakeholders. As Claverie & Kowalczuk (2022) highlight in their research on cyberpsychology, perceptions of cyber boundaries and interactions require an understanding of legal frameworks, cultural norms, and historical contexts.

By adapting the RIR governance model and geographic framework (Figure 1), CCoEs can establish clear cyber governance zones, define jurisdictional oversight over critical infrastructure, and standardize cybersecurity protocols. This structured alignment facilitates multinational coordination and strengthens regional cyber resilience against evolving threats.

3. Methodology for Operationalizing CCoEs

The establishment of multinational Cyber Centers of Excellence (CCoEs) is a critical step toward enhancing mission assurance in cyberspace. These centers can navigate diverse legal systems and strategic considerations while drawing inspiration from the RIR model to coordinate rapid responses to high-profile cyber incidents. While ambitious, the development of international cyber commons, cooperative cyber zones, cyber border controls, and governance structures could significantly improve global cybersecurity management.

A mixed-methods approach will guide CCoE implementation, integrating literature reviews, case studies, comparative analyses, expert interviews, conceptual modeling, and scenario planning. The literature review will examine existing cybersecurity governance structures, including the RIR system, international cyber law (e.g., Tallinn Manual), and national cybersecurity strategies. This will establish a foundation for leveraging regional cyber governance models to enhance collaboration among states and non-state actors.

A comparative analysis of cybersecurity strategies in the United States and the European Union will assess governance models, regulatory frameworks, and cyber defense policies, providing insights into geopolitical complexities and ensuring alignment with international standards. To identify best practices, a case study analysis will examine successful cyber cooperation initiatives, including the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), CISA's Joint Cyber Defense Collaborative (JCDC), and U.S. Cyber Command's Hunt Forward Operations (HFOs). These cases will highlight intelligence sharing, rapid response coordination, and regional cybersecurity training as foundational elements for CCoEs.

Semi-structured expert interviews with cybersecurity professionals, policymakers, and military officials will assess the feasibility, challenges, and implementation strategies for CCoEs. Insights from these interviews will inform conceptual modeling, defining cyber boundaries aligned with RIR regions, integration of public-private partnerships, and the role of proactive operations such as Hunt Forward missions in partner capacity-building efforts.

Scenario planning exercises will test the effectiveness of the CCoE framework against simulated cyber incidents and geopolitical crises, evaluating response times, intelligence-sharing efficiency, and mission assurance effectiveness. Once operational, CCoEs will be assessed based on information sharing, cross-border collaboration, cyber incident response times, attribution of malicious activities, and partner cyber defense capabilities. This methodology ensures that CCoEs function as trusted regional cybersecurity hubs, strengthening global cyber resilience, fostering international cooperation, and mitigating emerging cyber threats.

3.1 Building Trust for Mission Assurance

The 2007 cyber-attacks on Estonia underscored the need for multinational cooperation in cyberspace, demonstrating how a highly digitized society is vulnerable to coordinated cyber assaults (Ottis, 2008). This event led to the establishment of the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn, serving as a model for international collaboration. In response to legal ambiguities in cyberspace, the Tallinn Manuals emerged as living documents asserting that existing international law applies to cyber operations, referencing treaties such as the UN Charter, Geneva Conventions, and key case law (Cambridge, 2017; NSArchive, 2019). Though framed as lex lata (existing law) rather than lex ferenda (proposed law), the manuals remain subject to debate due to the evolving nature of cyber threats and limited state practice (Tanodomdej, 2019).

CCDCOE and similar entities already facilitate intelligence sharing and joint operations. Formalizing these arrangements into structured cooperative zones could enhance collective defense capabilities and coordinated responses to cyber threats. One approach involves establishing “digital customs checkpoints” at cyber borders to monitor data flows, detect malware, and enforce data localization laws. Alternatively, cyber demilitarized zones (DMZs) could serve as neutral monitoring areas, reducing accidental conflict escalation, fostering communication during cyber incidents, and allowing for third-party oversight. However, such measures could also deepen the digital divide between allied and non-allied nations, making shared interests a more viable foundation for cooperation.

A potential solution is designating critical internet infrastructure as an international cyber commons, shielding it from state interference. However, challenges arise due to private ownership, governance complexities, and enforcement difficulties (Global Commission, 2019). The Global Commission on the Stability of Cyberspace advocates protecting the “public core” of the internet, including undersea fiber-optic cables, which support global services such as cloud computing, GPS, and commerce. The 2022 Nord Stream pipeline sabotage further illustrates the intersection of cyber and physical security, highlighting the need for CCoEs to address both digital and physical vulnerabilities in critical infrastructure (Jones & Bachmann, 2022).

3.2 Bridging Gaps through Hybrid Threat Centers and Joint Collaboration

The Hybrid Threat Center (HTC) model, exemplified by the Australian-Lithuanian Cyber Research Network, provides a template for CCoEs to address complex threats (RMIT University, 2022). Modern cyber threats increasingly blur the lines between cyber, physical, and information warfare, necessitating a holistic, multidisciplinary approach to resilience. Most organizations lack the agility and civil-sector engagement needed for rapid, coordinated cyber responses. A Hybrid Threat Center model enables dynamic sourcing, training, and deployment of expertise tailored to regional cyber threats.

Partnerships are central to CCoE effectiveness. The Joint Cyber Defense Collaborative (JCDC), established by CISA, demonstrates how national initiatives can drive international cooperation (Mascellino, 2024). JCDC unifies cyber defenders across government and private sectors, a model that could be expanded within regional CCoEs to integrate international expertise.

Incident response in critical infrastructure sectors, such as water management or energy, often involves cross-border cooperation. JCDC focuses on defending against Advanced Persistent Threats (APTs), strengthening critical infrastructure security, and anticipating emerging threats (Mascellino, 2024). CCoEs, modeled after JCDC, could accelerate regional incident response times, enhance mitigation strategy sharing, and improve resilience against evolving cyber threats. By centralizing regional cybersecurity collaboration, CCoEs would reduce

response time for critical services restoration and strengthen infrastructure defenses against persistent cyber operations.

4. Mechanisms to Increase Partner Capacity in Cyberspace

The United States Cyber Command (USCYBERCOM) plays a critical role in cyberspace security cooperation, operating under statutory, fiscal, and policy mandates to strengthen cybersecurity partnerships with allied nations (USCYBERCOM, 2023). While geographic Combatant Commands (GCCs) lead most security cooperation activities, USCYBERCOM collaborates with them and the U.S. State Department to address regional cybersecurity concerns, integrating efforts into theater campaign plans to enhance international engagement (Larson, 2023).

Under the Unified Command Plan (UCP), Combatant Commanders (CCDRs) are responsible for planning, executing, and assessing security cooperation activities within their areas of responsibility (DoD, 2023). Joint Publication 3-20 emphasizes that Functional Combatant Commands (CCMDs) must develop integrated campaign plans, coordinating with GCCs, Service components, international organizations, and Security Cooperation Organizations (SCOs) (Joint Chiefs of Staff, 2017). DoD Directive 5132.03 further requires USCYBERCOM to align functional security cooperation plans with policy objectives and integrate them into theater campaign plans (DoD, 2016).

By aligning global cyberspace operations with GCC efforts, USCYBERCOM ensures effective coordination with the State Department and other agencies, positioning it to lead cybersecurity cooperation with nations that have advanced cyber capabilities. Integrating "country experts" from Cyber Centers of Excellence (CCoEs) into these efforts enhances cyber mission capacity and regional awareness, strengthening defenses against malicious cyber activities.

4.1 Operationalizing Trust in Cyberspace through Cooperation and Assistance

Security cooperation fosters defense relationships and enhances allied capabilities through training, cooperative research, and advisory support (DSCU, 2023). U.S. forces in contingency operations benefit from existing foreign access, expediting trust-building and enabling rapid, coordinated responses with regional expertise. These cyber-based capacity-building efforts, aligned with GCC, USCYBERCOM, and DoD missions, offer a cost-effective alternative to conventional military support.

However, navigating the legalities of operating in foreign networks remains a challenge due to varying authorities. This complexity hinders USCYBERCOM's ability to meet the increased demand for foreign interactions and ensure consistent partner engagements.

The National Defense Authorization Act (NDAA) funds security cooperation activities, including Operations and Maintenance (O&M) and program-specific initiatives. However, efforts like defense institution building and cyber capacity development often require additional funding beyond O&M. This research will examine additional funding mechanisms and their practical application to CCoEs to enhance international cyber cooperation and resilience.

Table 1 categorizes key mechanisms for military-to-military engagements and training with foreign forces. It details authorities enabling operational exchanges (164), international personnel exchanges (311), funding for theater security cooperation (312), and joint training with foreign military forces (321). These authorities enhance security cooperation by facilitating knowledge exchange, improving interoperability, strengthening alliances, and bolstering regional cyber resilience. By leveraging these mechanisms within USCYBERCOM, a CCoE can build trusted partnerships, enhance collective cyber defense capabilities, and ensure a coordinated approach to emerging cyber threats.

Table 1: USCYBERCOM's Security Cooperation Authorities under Title 10

		Authority	Type	Summary	Examples
TITLE 10	Military -to- Military	164	Powers & Duties of the Combatant Commander	CCDs authorized to use O&M to conduct traditional mil-to-mil activities. Events are short in duration and do not cross into capacity	- Staff talks - Seminars - Conferences - Info Exchange SMEES - Advise & Assist
		311	Exchanges of defense personnel between the U.S. & friendly foreign	Authority to enter into international exchange agreements for the purpose of exchanging members of the armed forces and civilian personnel of the defense or security ministry of that foreign government or international or regional security organization.	- Instructors - Research & Development personnel
		312	Payment of personnel expenses necessary for theater security cooperation	Authority to pay for friendly foreign governments and non-governmental personnel expenses necessary for mission-related theater security cooperation activities supporting U.S. interests.	- Seminars - Conferences - SMEES - Travel

		Authority	Type	Summary	Examples
	Training with Foreign Forces	321	Training with friendly foreign countries; payment of training and exercise expenses	Authority to train with the military/security forces of a friendly foreign country, and to pay training and exercise expenses.	- Any joint U.S. training with foreign partners - Annual exercises

Note. Adapted from Larson (2023).

Table 2 focuses on support for operations, capacity building, and education & training activities. It details authorities for operational support to friendly foreign forces (331), defense institutional capacity building (332), and partner force development through training and equipment (333). Additionally, it includes training authorities for foreign military personnel (321) and distribution of education and training materials to enhance interoperability (346). These mechanisms enhance cyber cooperation by improving interoperability, strengthening partner capacity, and facilitating joint training initiatives. By leveraging these USCYBERCOM authorities, CCoEs can bolster allied cyber capabilities, enhance regional security, and promote a coordinated approach to cyber defense.

Table 2: USCYBERCOM's Security Cooperation Authorities under Title 10

		Authority	Type	Summary	Examples
TITLE 10	Support For Ops & Capacity Building	331	Friendly foreign countries: authority to provide support for the conduct of operations.	Provide support (logistics, supplies, services) to forces of a friendly foreign country participating in: an operation with the armed forces of the DOD military/ stability operations that benefit US national security interests; and/or solely for the purpose of enhancing interoperability of forces in a combined operation.	- Logistical support - Supplies Services - Procurement of equipment for loan to friendly force - Specialized training
		332	Friendly Foreign Countries; International & Regional Organizations: Defense Institutional Capacity Building (DIB)	Ministry of Defense Advisor (MODA) Authority. Allows SMEs, civilian advisors. and other expertise in helping a respective country's MOD and/or various security agencies with DIB. Not likely to be executed/accessed by USCYBERCOM.	- MODA - Strategic planning - Training for MOD
		333	Foreign Security Forces: Authority to Build Partner Capacity	Authority to conduct/support a programs) to provide training & equipment to the national security forces of 1+ countries for building capacity. USCYBERCOM may execute under this authority only in support of a GCC significant security cooperation initiative.	- Education - Training - Services - Equipment

		Authority	Type	Summary	Examples
	Education & Training Activities	321	Training with friendly foreign countries; payment of training and exercise expenses	Authority to train with military / security forces of a friendly foreign country, and to pay training and exercise expenses.	- Any joint U.S. training with foreign partners - Annual exercises
		346	Distribution to Certain Foreign Personnel of Education and Training Material and Informational Technology to Enhance Military Interoperability with the Armed Forces	International students enroll in DOD distance learning courses.	- Education - Training

Note. Adapted from Larson (2023).

Security assistance refers to a group of programs authorized by the Foreign Assistance Act of 1961, through which the U.S. provides defense articles, military training, and other defense-related services to foreign nations (DSCU, 2023). This assistance can be delivered via grants, loans, cash sales, or leases, aimed at furthering U.S. national policies and objectives. The Department of State primarily oversees these programs under Title 22 authorities, which include various forms of military aid and training initiatives designed to enhance the capabilities of allied nations (DSCU, 2023). According to DOD Directive 5132.03, security cooperation aims to provide U.S. forces with access to friendly foreign countries during peacetime and in contingency operations.

Table 3 focuses on defense trade, arms transfers, and countering foreign influence. It includes authorities for Foreign Military Sales (FMS), allowing eligible governments to purchase U.S. defense articles, services, and training, and the Foreign Military Financing Program (FMFP), which provides grants and loans for these purchases. The International Military Education & Training (IMET) program funds professional military education for foreign personnel. Additionally, the Countering PRC Influence Fund (CCIF) and Countering Russian Influence Fund (CRIF) provide grant assistance to enhance security cooperation, counter foreign influence, and build partner capacity.

Table 3: USCYBERCOM's Security Assistance Authorities under Title 22

	Authority	Type	Summary	Examples
TITLE 22 Defense Trade & Arms Transfers	FMS	Foreign Military Sales	A non-appropriated program administered by DSCA through which eligible foreign governments purchase U.S. defense articles, services, & training. SCOs play the primary role in initiation of an FMS case.	-Purchasing government pays associated costs
	FMFP	Foreign Military Financing Program	The program consists of congressionally appropriated grants and loans, which enable eligible foreign governments to purchase U.S. defense articles, services, & training.	- Can be used by eligible countries to fund FMS cases.
	IMET	International Military Education& Training	Provides grant financial assistance for training in the U.S. and, in some cases, in overseas facilities to selected foreign military and civilian personnel.	- Funds foreign professional military education.
	CCIF	Countering PRC Influence Fund	Provides grant assistance partially executed under FMFP & IMET to counter the influence of the Government of the People's Republic of China and the Chinese Communist Party and entities acting on their behalf globally.	- Can be used by eligible countries to purchase U.S. defense articles, services & training.
	CRIF	Countering Russian Influence Fund	Provides grant assistance partially executed under FMFP & IMET to enhance capacity of law enforcement and security forces in Europe, Eurasia, and Central Asia and strengthen security cooperation between such countries and the United States & NATO	- Can be used by eligible countries to purchase U.S. defense articles, services & training.

Note. Adapted from Larson (2023).

Coordinating with a CCoE that reviews opportunities for additional authorities, forces, and funding lines supports the growing demand for foreign partner engagements, reducing USCYBERCOM's planning and coordination requirements. The authorities under Title 10 and Title 22 can guide a regional CCoE's efforts in coordinating with USCYCBERCOM cyber forces for various cyberspace support and missions. Security assistance and security cooperation are critical components of U.S. foreign policy, particularly in the context of defense and military operations. These authorized programs provide substantial governance for military and foreign relations, perhaps forging the requirement for CCoEs to increase partner capacity to defend in cyberspace.

4.2 Enhancing Partner Cybersecurity Capacity with Forward Cyberspace Operations

In the context of U.S. Cyber Command's (USCYBERCOM) Hunt Forward Operations (HFOs), leveraging Titles 10 and 22 is particularly significant. HFOs are strictly defensive cyber operations conducted at the request of partner nations. When invited, USCYBERCOM deploys Hunt Forward Teams to partner countries to observe and detect malicious cyber activities on their networks (U.S. Cyber Command Public Affairs, 2022). This operation not only enhances the cybersecurity posture of partner nations but also generates valuable insights that bolster U.S. homeland defense. The DoD Cyber Strategy also emphasizes "defending forward" to disrupt or halt malicious cyber activities at its source (DoD Cyber Strategy, 2018).

HFOs are staffed exclusively by personnel from USCYBERCOM's Cyber National Mission Force (CNMF), who are specially trained to secure and defend the Department of Defense Information Network (DODIN) against cyber threats. CCoEs can provide the conduit for partners to integrate into USCYBERCOM designated Hunt/Defend Forward Teams, quickly detecting malicious activities on host nation networks. CCoEs provide critical data that can inform broader cybersecurity strategies enhancing the resilience of shared networks against cyber threats. Understanding the cyber threat further highlights the need for agreements centered on trust and exclusivity to share operationally relevant information and regional intelligence.

5. Building Trust and Cyber Capacity through Strategic Sharing

The Five Eyes (FVEY) intelligence alliance—comprising Australia, Canada, New Zealand, the United Kingdom, and the United States—serves as a strategic model for intelligence sharing that CCoEs can emulate (Corbett & Danoy,

2022). Like FVEY, CCoEs can contribute intelligence from their regions, leverage privileged access, and extend partnerships to counter cyber threats.

Automated Indicator Sharing (AIS), operated by CISA, provides a framework for real-time cyber threat intelligence (CTI) sharing using standardized formats like STIX and TAXII (CISA, n.d.). CCoEs can adopt AIS protocols to enhance interoperability, transparency, and trust among regional partners. Similarly, the Federal Multilateral Information Sharing Agreement (MISA) facilitates machine-speed cybersecurity data exchange across U.S. federal agencies, establishing responsibilities and trust mechanisms (DHS, 2019). CCoEs can leverage such agreements to unify threat detection, incident response, and mitigation strategies within regional cybersecurity frameworks.

These agreements also prioritize privacy and civil liberties protections. AIS, for example, removes personally identifiable information (PII) unrelated to cyber threats and enforces data retention limits (CISA, n.d.). By adopting similar safeguards, CCoEs can establish a privacy-conscious intelligence-sharing ecosystem, fostering secure and collaborative cybersecurity partnerships.

6. Conclusion

Different geopolitical alliances could define and manage their cyber boundaries through a multifaceted strategy focused on robust intelligence sharing and regional Cyber Centers of Excellence (CCoEs). By aligning cyber defense resources with critical infrastructure and fostering collaborative intelligence gathering, alliances enhance their ability to detect and respond to cyber threats. This approach clarifies roles and responsibilities across allied networks, ensuring swift and coordinated countermeasures.

Integrating multiple CCoEs into a unified framework strengthens interoperability and mission assurance, enabling alliances to address hybrid warfare threats more effectively. By reducing operational ambiguity and exposing actors engaged in gray zone activities, this strategy deters potential adversaries while adapting to the evolving cyber landscape. These enduring partnerships reinforce a collective commitment to cybersecurity, presenting a unified and resilient front against emerging threats.

References

Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law, 21*(2), 245–272.

Cambridge University Press. (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. https://assets.cambridge.org

Christophe, J.-P. (2020). Defending forward in cyberspace and the case for transparency. *Marine Corps University, Command and Staff College*. https://apps.dtic.mil/sti/pdfs/AD1177547.pdf

Claverie, B., & Kowalczuk, B. (2022). Cyberpsychology. In B. Claverie, B. Prébot, N. Buchler, & F. Du Cluzel (Eds.), *Cognitive warfare: The future of cognitive dominance* (pp. 9–1 – 9–5). NATO Science and Technology Organization. https://hal.science/hal-03635933

Corbett, S., & Danoy, J. (2022, October 31). Beyond NOFORN: Solutions for increased intelligence sharing among allies. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-noforn-solutions-for-increased-intelligence-sharing-among-allies/

Creemers, R. (2020). *China's approach to cyber sovereignty*. Konrad Adenauer Stiftung.

Cybersecurity and Infrastructure Security Agency. (n.d.). Automated indicator sharing (AIS) 2.0 documents & more information. Retrieved February 16, 2025, from https://www.cisa.gov/automated-indicator-sharing-ais-20-documents-more-information

Defense Security Cooperation University. (2023). *Security cooperation programs handbook: Fiscal year 2023*. Defense Security Cooperation Agency, Department of Defense.

Department of Defense. (2016). *DoD Directive 5132.03: DoD policy and responsibilities relating to security cooperation*. https://open.defense.gov/portals/23/Documents/foreignasst/DoDD_513203_on_Security_Cooperation.pdf

Department of Defense. (2018). *DoD cyber strategy*. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Department of Defense. (2023). *2022 Unified Command Plan*. Federal Register. https://www.federalregister.gov/documents/2023/04/28/2023-09182/2022-unified-command-plan

Department of Homeland Security. (2019). *Federal multilateral information sharing agreement*.

Global Commission on the Stability of Cyberspace. (2019). *Advancing cyberstability: Final report*. https://cyberstability.org/assets/images/report/GCSC-Advancing-Cyberstability.pdf

Harold, S. W., Libicki, M. C., & Cevallos, A. S. (2016). *Getting to yes with China in cyberspace*. RAND Corporation.

Hill, R. (2016). Internet governance, multi-stakeholder models, and the IANA transition: Shining example or dark side? *Journal of Cyber Policy, 2*(2), 176–197. https://doi.org/10.1080/23738871.2016.1227866

Hoffmann, S., Lazanski, D., & Taylor, E. (2020). Standardising the splinternet: How China's technical standards could fragment the internet. *Journal of Cyber Policy, 5*(2), 239–264. https://doi.org/10.1080/23738871.2020.1805482

Joint Chiefs of Staff. (2017). *Joint Publication 3-20: Security cooperation*. https://irp.fas.org/doddir/dod/jp3_20.pdf

Jones, M. P., & Bachmann, S. D. (2022, October 4). 'Hybrid warfare': Nord Stream attacks show how war is evolving. *The Conversation*. https://theconversation.com/hybrid-warfare-nord-stream-attacks-show-how-war-is-evolving-191764

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review, 107*(2), 326–343.

Larson, A. (2023). *USCYBERCOM security cooperation authorities* [Information paper].

Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. *International Security, 39*(3), 7–47.

Lysne, O. (2018). *The Huawei and Snowden questions: Can electronic equipment from untrusted vendors be verified?* Springer.

Mascellino, A. (2024, February 13). CISA reveals JCDC's 2024 cybersecurity priorities. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/cisa-reveals-jcdc-2024/

Ministry of Foreign Affairs of the People's Republic of China. (2020). *Global Initiative on Data Security*.

NSArchive. (2019). *Tallinn Manual 2.0 in the international law applicable to cyber operations*. https://nsarchive.gwu.edu

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. *Cooperative Cyber Defence Centre of Excellence*.

Regional Internet Registry System. (2022). *The RIR system: How it works*. https://www.nro.net

RMIT University. (2022). RMIT University launches Australia's first Hybrid Threat Centre between Australia and Lithuania. https://www.rmit.edu.au/news/ccsri/hybrid-threat-centre-launched

Sacks, S. (2018). New China data privacy standard looks more far-reaching than GDPR. *Center for Strategic and International Studies*.

Tanodomdej, P. (2019). The Tallinn Manuals and the making of cyber law. *Masaryk University Journal of Law and Technology, 13*(1), 61–86.

U.S. Cyber Command. (2023). *2023 posture statement of General Paul M. Nakasone*. https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone/

U.S. Cyber Command Public Affairs. (2022, November 15). *Cyber 101: Hunt forward operations*. 960th Cyberspace Wing. https://www.960cyber.afrc.af.mil/News/Article-Display/Article/3219164/cyber-101-hunt-forward-operations/

U.S. Department of State. (2020). *The Clean Network*.