COLUMBIA | SIPA
School of International and Public Affairs

CDAC
A CRDF GLOBAL INITIATIVE

Assessing the Effectiveness of Cyber Defense Assistance

June 2024

Contents

Overview 04

Purpose, Scope and Methodology 05

Background 06

Development of Evaluation Framework 08

Existing Frameworks 08

Expert Interviews 10

Proposed Framework 11

Operational Success 16

Efficiency 18

Strategic Planning 18

Friction 21

Sustainability 22

Framework Implementation and Recommendations 23

Lessons Learned 24

Conclusion 27

Appendices 28

References 35

Columbia SIPA Capstone Team

Charlotte Lin
Carlos Reyna
Jack Frew
Olivia Adams
Pat Aungsusuknarumol
Seamus Boyle
Tarang Jain

Special Thanks

Daniel Dobrygowski
Adjunct Associate Professor of International and Public Affairs, Columbia SIPA

Greg Rattray
Executive Director, Cyber Defense Assistance Collaborative (CDAC)

Seungmin (Helen) Lee
Program Associate, Cyber Defense Assistance Collaborative (CDAC)

Nadia Amrani
Graduate Student, Columbia SIPA

Published May 2024
Columbia University | School of International and Public Affairs

Overview

The ongoing war in Ukraine represents a significant evolution of modern warfare, with a Russian military invasion on the ground accompanying cyberattacks on critical infrastructure and information warfare in the digital realm. Yet, Russia's cyber offensive has had limited success against Ukrainian networks, partly due to private sector-led Cyber Defense Assistance (CDA): technology and cybersecurity companies have come together to provide Ukraine with ongoing support, including cyber threat intelligence, tools, services, and training to defend Ukraine's digital environment.

One organization at the forefront of CDA in Ukraine is the Cyber Defense Assistance Collaborative (CDAC). As the digital battleground expands, lessons learned by CDAC, and its public-private partnerships are imperative to understand the capability gaps and path forward for providing CDA. Despite years of CDA provision to Ukraine, the question of assessing CDA's effectiveness remains. Thus, this report presents a novel evaluation framework for measuring CDA effectiveness.

Based on relevant open-source research and a review of existing evaluation frameworks in areas such as cybersecurity, defense assistance, and foreign and development aid, the resulting framework identifies 13 components and 33 indicators across five key pillars: *Operational Success, Efficiency, Strategic Planning, Friction* and *Sustainability*. The framework provides a three-phased approach designed to enable users to prioritize certain aspects of evaluation - operational, strategic, and organizational - at different points of conflict and CDA provision.

Ultimately, the evaluation framework provides several approaches to implementation including assessment of existing data, identification of knowledge gaps, and proposed metrics and concepts to improve operating processes for CDA provision. Additional lessons learned from the process of framework building include the importance of a sequenced approach tailored to local expertise and needs and recognizing the importance of building trust among CDA providers and recipients. In the face of future conflicts, this framework can help to refine and assess the effectiveness of CDA to defend nations under attack in the cyber domain.

Purpose, Scope and Methodology

This report aims to provide a framework to evaluate CDA effectiveness. After two years of CDA to Ukraine, CDAC's ongoing convenings of a wide range of governmental and private sector stakeholders indicate that no organization or government has a deep understanding of how to assess the effectiveness of these activities. The framework presented in the report highlights components that must be considered when evaluating CDA. The report seeks to inform interested stakeholders on enhancing CDA delivery, prioritizing efforts, and understanding the broader applications of CDA to future conflicts.

The scope of the project includes:

- identification of key components and indicators that assess the effectiveness of CDA
- analysis of the cyber defense landscape and assistance to Ukraine since Russia's invasion
- development of a framework applicable to different contexts and time periods

The methodology involved open-source research and expert interviews to develop a five-pillar framework that measures the effectiveness of CDA:

- **Open-Source Research:** included a review of existing frameworks, policy documents, and reports related to the effectiveness of cybersecurity, defense assistance, foreign aid, and development assistance. Existing frameworks included the OECD Overseas Development Assistance for the field of foreign aid and development assistance, MITRE's framework for cyber resiliency, and accounts of defense aid evaluation from the RAND Corporation and the United States (US) government. This review provided a list of elements that would apply to the context of CDA. The review of reports and research papers also provided an understanding of the post-invasion cyber threat landscape in Ukraine.
- **Interviews**: 11 expert interviews were conducted with CDAC staff, CDAC-affiliated providers, Ukrainian coordinators involved in connecting providers to recipients, and cybersecurity experts. The interviews helped identify the challenges faced in delivering and receiving aid and provided insight into the factors that could be incorporated into the evaluation of CDA effectiveness.

Background

Defense assistance and development aid have long been integral to diplomacy. However, the field of CDA was relatively unexplored until the war in Ukraine began. Western states and private sector firms have provided over US $450 million in CDA to Ukraine as of mid-2024.[1] Given the private sector's cyber capabilities and ability to mobilize rapidly, CDA necessitated private-public cooperation, as well as a framework to evaluate the effectiveness of this type of assistance.[2] Table 1 illustrates the cyber landscape in Ukraine following the 2022 Russian invasion.

Table 1: Key Cyber Developments in Ukraine following the 2022 Russian Invasion

Date	Incident/Initiatives	Description/Impact
January 13, 2022	WhisperGate	Wiper malware found on systems throughout Ukraine, including the Foreign Ministry and networks used by the Ukrainian cabinet.[3]
February 23, 2022	HermeticWiper	Wiper spread beyond the borders of Ukraine and may have affected some systems in Baltic countries.[4]
February 24, 2022	Viasat	A cyberattack disrupted broadband satellite internet access on the day of Russia's invasion.[5]
February 28, 2022	Starlink Activation	SpaceX activated its Starlink satellite internet service in Ukraine, providing alternative communication and internet amidst cyberattack-induced disruptions. The Starlink terminals ensured internet connectivity, supporting essential services, government operations, and civilian communications during the war.[6]
December 12, 2023	Kyivstar	A cyberattack by Russian hackers on Kyivstar, Ukraine's largest telecom provider, that disrupted mobile signals and internet for millions, damaging network infrastructure. The attack affected services including air raid sirens, banks, and payment systems.[7]
February 8, 2024	Ukraine Discloses Cyber Operations in Russia	Ukraine's Security Service (SBU) and Main Directorate of Intelligence of the Ministry of Defense (HUR) conducted cyber operations against major Russian targets, including Alfa-Bank, compromising over 30 million customer records; Rosaviatsia, disrupting aviation operations; "Planeta," destroying databases and equipment; and the FNS, where over 2,300 servers and a tech firm managing its databases were compromised.[8]

Shortly after the conflict began, CDAC emerged as a crucial player for CDA in Ukraine. Composed of leading cybersecurity firms, former US government officials, and top cyber defense leaders, CDAC has been instrumental in operationalizing CDA through targeted support activities, including threat intelligence, technology provision, training, and advisory services[9] with an estimated value of over $30 million.[10] CDAC's model and approach to CDA may be needed in a potential future conflict, such as a Taiwan Strait Crisis. In a future conflict, CDA could be more effectively delivered if lessons learned by CDAC can be leveraged—one of which is establishing and utilizing a framework that measures CDA effectiveness.

Development of Evaluation Framework

Existing Frameworks

Given the novelty of CDA in conflict zones, evaluation frameworks do not yet exist. Thus, this report first draws from existing frameworks and research across various domains including:

- RAND Corporation's Making Military Aid Work [11]
- US Department of State's Stabilization Assistance Review: A Framework for Maximizing the Effectiveness of U.S. Government Efforts to Stabilize Conflict-Affected Areas [12]
- Organization for Economic Co-operation and Development's (OECD) Applying Evaluation Criteria Thoughtfully [13]
- MITRE's Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring [14]
- The World Bank's Where to Spend the Next Million? Applying Impact Evaluation to Trade Assistance [15]
- National Institute of Standards and Technology (NIST) Framework Cybersecurity Framework 2.0 [16]

The existing frameworks highlight the importance of successful strategic planning and operations, sustainability, and efficiency:

- NIST, RAND, and MITRE frameworks illustrate the importance of strategic and operational aspects.
- The World Bank and OECD's findings on diminishing returns for aid point to the importance of sustainability and efficiency.
- The State Department's SAR emphasizes the importance of institutionalizing accountability through information flows.

Table 2 summarizes the similarities, differences, and applicability of these evaluation and cybersecurity frameworks to CDA evaluation.

Table 2: Summary of Evaluation Frameworks and their Applicability to a CDA Evaluation Framework

Framework	Strengths	Weaknesses	Applicability to CDA Evaluation
Defense Aid (RAND)	Analyzes successes and failures of aid based on planning, priority targets, and nature of relationships with recipients.	Risk of oversimplifying defense aid regimes with three categories.	Highlights the benefits of prioritizing recipient needs and effective tools for institutional reform.
US Department of State Stabilisation Assistance Review (SAR)	Assesses stabilization efforts in conflict-affected countries and leveraging US diplomatic, defense, and foreign assistance resources.	Primarily focuses on public sector (US government) efforts in post-conflict areas.	Importance of sequenced and targeted assistance for self-reliance. Mechanisms to institutionalize evaluation and accountability.
OECD Overseas Development Assistance (ODA)	Provides a holistic framework with six criteria, including examples for practical implementation.	Specific orientation towards country priorities and diplomatic goals.	Offers a broader evaluative lens that extends beyond technical capabilities to include the socio-economic impacts and strategic alignment of aid.
MITRE metrics for cyber resiliency and effectiveness	Outlines four pillars to assess the efficacy of cybersecurity technology: capability, practicality, quality, and provenance.	Assesses effectiveness from a vendor-recipient lens.	Benchmarks cybersecurity practices against standards, providing quantitative evaluation of technical resilience.
The World Bank	Emphasizes multilateral engagement for effective aid distribution, ensuring proportional and equitable distribution of aid relative to economic and population growth factors.	Randomized Control Trials (RCTs) impractical in conflict zones due to unpredictability.	Economic assistance models aid in assessing allocation efficiencies and ensuring CDA is proportionate to recipient organization needs.
NIST Cybersecurity Framework (CSF) 2.0	Evaluates operational, strategic and organizational aspects of cybersecurity. Intended to be used by organizations regardless of the maturity level of their cybersecurity programs.	Large focus on organizational cybersecurity governance.	Provides a taxonomy of high-level cybersecurity outcomes , emphasis on risk management and concurrent assessment of interrelated functions to prioritize efforts effectively.

Expert Interviews

Eleven interviews with CDA, cybersecurity, and cyber capacity-building experts supplemented the findings from existing evaluation frameworks. While the interview findings primarily reflected experiences in Ukraine, they offered unique insights into aspects of CDA that open-source research failed to address. For instance, interviews with aid providers highlighted the importance of adaptability and the flexibility of CDA strategies given the dynamic nature of cyber threats. Table 3 summarizes the findings from the expert interviews.

Table 3: Key Findings and Implications for CDA from Interviews [17]

Critical Area	Observation	Implications for CDA Evaluation
Importance of Historical Presence in Ukraine	A historical presence or prior engagement in Ukraine is crucial for understanding the context and effectively tailoring assistance.	Establishing long-term relationships and a deep understanding of the local environment will be key for operational success. This suggests a strategic emphasis on building and maintaining presence well before crises emerge.
Need for a Feedback Loop and Greater Transparency	There is a wide consensus on the need for transparency reporting when it comes to CDA. The absence of a systematic feedback loop and transparency in operations hampers the ability to assess and adapt cyber assistance effectively.	Developing mechanisms for regular, structured feedback from recipients and ensuring transparency in CDA operations are vital. This may involve creating dedicated channels for feedback, appointing teams to analyze feedback, and integrating findings into ongoing planning and execution.
Sustainability Issues	Challenges in sustaining funding and volunteer efforts hinder CDA effectiveness and are exacerbated by the difficulty of measuring the impact and sustainability of assistance.	Identifying sustainable funding sources and models for volunteer engagement is critical.
Operational Friction	Lack of standard operating procedures (SOPs), time zone differences, language barriers, and reliance on volunteers, create friction in the delivery and implementation of assistance.	Developing SOPs, considering multilingual support, and establishing clear roles and schedules can mitigate these operational challenges. Enhanced training and support for volunteers may also improve efficiency and reduce friction.
Challenges to Measuring Effectiveness of Cybersecurity	Complex nature of cyber conflict makes it difficult to measure the effectiveness of CDA and attribute outcomes directly.	Developing metrics that account for indirect and long-term effects of CDA.
Volunteer and Participant Fatigue	Ongoing conflict and prolonged assistance without compensation leads to fatigue among CDA personnel and coordinators, affecting commitment and participation.	Addressing volunteer and participant fatigue requires attention to well-being, compensation models (where applicable), and rotation schemes.

Proposed Framework

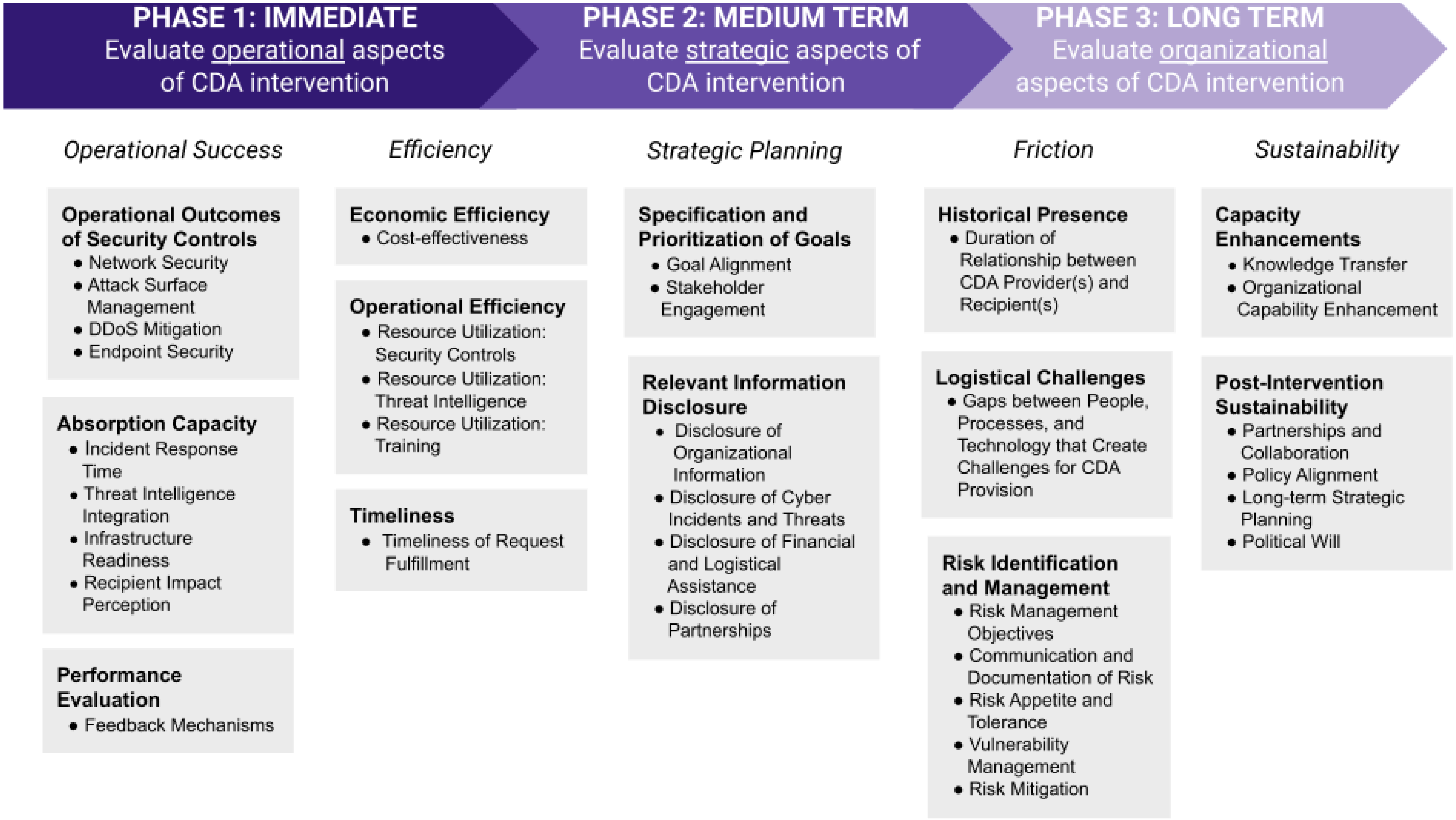
Overview

The framework for evaluating the effectiveness of CDA integrates traditional benchmarking methodologies with a mixed-methods approach that includes both quantitative and qualitative metrics. The framework considers the inherent challenges of limited resources and the urgent need for assistance at the conflict's outset, thereby providing an approach that prioritizes evaluating key aspects of CDA at specific points in the conflict and provision timeline:

- **Phase 1: Immediate**
  - Evaluates the operational aspects of CDA intervention.
  - Conflict is in the early stages and/or CDA provision has recently begun.
- **Phase 2: Medium-term**
  - Evaluates the strategic aspects of CDA intervention.
  - Conflict is escalating and CDA interventions are being scaled up.
- **Phase 3: Long-term**
  - Evaluates the organizational aspects of CDA intervention.
  - Conflict is ongoing and CDA intervention is established, or a reduction is expected in the near future.

This framework is structured around five pillars: *Operational Success, Efficiency, Strategic Planning, Sustainability*, and *Friction*. Each pillar is broken down into multiple components, with specific indicators identified for these components, as shown in Figure 1.

Figure 1: Proposed Evaluation Framework [18]



PHASE 1: IMMEDIATE
Evaluate operational aspects of CDA intervention

Operational Success

Operational Outcomes of Security Controls
- Network Security
- Attack Surface Management
- DDoS Mitigation
- Endpoint Security

Absorption Capacity
- Incident Response Time
- Threat Intelligence Integration
- Infrastructure Readiness
- Recipient Impact Perception

Performance Evaluation
- Feedback Mechanisms

Efficiency

Economic Efficiency
- Cost-effectiveness

Operational Efficiency
- Resource Utilization: Security Controls
- Resource Utilization: Threat Intelligence
- Resource Utilization: Training

Timeliness
- Timeliness of Request Fulfillment

PHASE 2: MEDIUM TERM
Evaluate strategic aspects of CDA intervention

Strategic Planning

Specification and Prioritization of Goals
- Goal Alignment
- Stakeholder Engagement

Relevant Information Disclosure
- Disclosure of Organizational Information
- Disclosure of Cyber Incidents and Threats
- Disclosure of Financial and Logistical Assistance
- Disclosure of Partnerships

PHASE 3: LONG TERM
Evaluate organizational aspects of CDA intervention

Friction

Historical Presence
- Duration of Relationship between CDA Provider(s) and Recipient(s)

Logistical Challenges
- Gaps between People, Processes, and Technology that Create Challenges for CDA Provision

Risk Identification and Management
- Risk Management Objectives
- Communication and Documentation of Risk
- Risk Appetite and Tolerance
- Vulnerability Management
- Risk Mitigation

Sustainability

Capacity Enhancements
- Knowledge Transfer
- Organizational Capability Enhancement

Post-Intervention Sustainability
- Partnerships and Collaboration
- Policy Alignment
- Long-term Strategic Planning
- Political Will

Using the Evaluation Framework

For data collection, evaluators of CDA can gather information using both direct and proxy indicators. Where quantitative data is unavailable to measure a specific indicator, the framework relies on proxy indicators. These indicators are assessed primarily through survey questions distributed to stakeholders who rate their perceptions on a scale from 1 to 5 for each indicator. This process can provide an aggregated score reflecting stakeholders' alignment with the indicators.

This approach systematically assesses CDA, highlighting areas where data collection efforts should be intensified, particularly in instances where data accessibility is limited. Recognizing the challenges in quantifying certain metrics, the framework includes scaled descriptions for each survey question to standardize measurement. By employing this mixed-methods approach, the framework not only evaluates current performance but also guides CDA stakeholders in developing better reporting metrics to accurately assess their cyber defense capabilities.

Data Aggregation and Analysis: Using Direct and Proxy Indicators

Ideally, each indicator would quantitatively measure how well CDA interventions are performing. However, in cases where direct measurements are not available — due to confidentiality, operational security, or complexities of quantifying effectiveness in cybersecurity — proxy indicators become essential. [19] Proxy indicators can provide valuable insights into the perceived and indirect impacts of cybersecurity measures, bridging gaps when direct data collection is either impractical or impossible. Of the 33 total indicators, 19 have both direct and proxy indicators of measurement, while 3 have exclusively direct indicators and 12 exclusively proxy indicators. The use of both direct and proxy indicators across pillars and components allows the evaluator to develop a more nuanced understanding. Table 4 demonstrates how proxy indicators can complement direct indicators in a synthesized evaluation or be used exclusively.

Table 4: Explanation of Synthesized Evaluation Process

Indicator	Director Indicator	Proxy Indicator
Knowledge transfer	*The total number of participants attending cybersecurity training sessions increased by 15% across all recipient organizations in the last year.*	*On average, recipients scored this indicator 4.38 out of 5, indicating a high level of knowledge transfer between provider and recipient.*
DDoS mitigation	*The mean time to respond (MTTR) to DDoS attacks fell by 25% in the year after security controls were initially provided.*	
Relevance of provided threat intelligence		*On average, recipients scored this indicator 2.51, suggesting provided threat intelligence was somewhat relevant to the security of their environment.*

Analysis of Direct Indicators

CDA stakeholders evaluating their interventions should self-benchmark by tracking each direct indicator over different time periods to establish internal benchmarks and monitor trends. This process helps to observe progress or regression in specific metrics over time. Separate analyses should be conducted for each indicator to understand its contributions to the broader objective. For instance, evaluating the annual change in training numbers and independently assessing variations in incident rates or attack severity provides clear insights into the specific areas of improvement or concern.

Integrating insights from direct indicators with those from proxy indicators can enhance the credibility of the analysis by validating quantitative data with qualitative perceptions. Statistical tools can be employed to correlate changes in direct indicators with outcomes reported by proxy indicators, establishing an empirical basis to potentially infer causality and attribute effectiveness.

Analysis of Proxy Indicators

A Likert scale assessment strategy was used for proxy indicators. The scale (1 to 5) aims to capture the perceived impact of CDA stakeholders. This method reduces informational errors by confining responses to a predefined scale with each score on the scale — 1 signaling the least desirable outcome to 5 indicating the most desirable — clearly defined to ensure uniform interpretation across respondents. [20]

The analysis dashboard (outlined in Appendix 2) uses a three-color gradient system to visually reflect the nuances in performance derived from survey responses:

- **Shades of red:** indicate a skew towards 1, highlighting areas requiring urgent improvement.
- **Shades of yellow:** illustrate a score around 2.5, indicating moderate effectiveness with potential for enhancement.
- **Shades of green:** denote scores approaching 5, signifying strong performance.

Additionally, standard deviation serves as an additional analytical tool offering insights into the consensus level among respondents.[21]

- **Standard deviation below 1:** Indicates strong consensus with minimal variability.
- **Standard deviation from 1 to 1.5:** Suggests moderate variability.
- **Standard deviation above 1.5:** Highlights significant disagreement.[22]

Limitations of the Proposed Evaluation Framework

The proposed evaluation model does present inherent limitations such as:

- **Rating Scale:** Proxy indicators, including survey questions with pre-filled descriptions, may oversimplify complex issues and fail to capture nuances, potentially reducing the depth of analysis.
- **Subjectivity in Indicator Selection:** Deciding on indicators and setting thresholds for survey questions introduces subjectivity, affecting evaluation outcomes and reflecting the biases of evaluation designers.
- **Need for Adaptability and Evolution:** Given the dynamic nature of cybersecurity threats, the framework requires ongoing updates and a flexible revision process to maintain relevance over time.
- **Proxy Indicators**: Given the challenges of directly measuring certain aspects of cybersecurity effectiveness, such as the efficacy of tools in deterring or preventing cyberattacks, numerous indicators in the framework serve as proxies. These proxy indicators largely capture the enabling environment of CDA effectiveness, rather than directly measuring the aspect of CDA effectiveness at hand.
- **Need for Continuous Stakeholder Engagemen**t: The framework emphasizes stakeholder engagement, requiring data collection from CDA stakeholders. However, this participatory approach poses challenges due to the additional labor required for data collection and analysis.

The Framework's Five Pillars

The framework's five pillars comprehensively evaluate CDA effectiveness by examining operational, strategic, and organizational aspects across different time periods. These pillars offer a means to prioritize specific aspects of evaluation while also presenting a temporal view of effectiveness, emphasizing the interrelated nature of all pillars. Variations in the size of the pillars reflect their differing impact on overall effectiveness, as determined by interview findings and analysis of the CDAC experience in Ukraine. The following section provides an overview and rationale of each pillar and its components, detailing how each contributes to the holistic framework and can be applicable to any CDA intervention.

Operational Success

The *Operational Success* pillar is deemed one of the most critical elements of evaluation and is prioritized in the evaluation framework under **Phase 1: Immediate**. Stakeholders may differ on the relative importance of different pillars, however, if the CDA does not serve the immediate needs of recipients, the CDA is ineffective. The *Operational Success* pillar consists of three key components, as described below:

- **Operational Outcomes of Provided Security Controls:** Metrics gathered through provided security control software and technology can serve as quantitative evidence of the operational success of CDA. The insights provided by network security, attack surface management, DDoS mitigation, and endpoint security tools can serve as indicators for the success of CDA in deterring or mitigating attacks.
- **Absorption Capacity**: The effectiveness of CDA relies largely on how well recipients can receive and implement assistance. Metrics like incident response time and evaluations of integrating threat intelligence, infrastructure readiness, and the perceived impact on recipients all gauge the capacity to absorb CDA.
- **Performance Evaluation:** Operational success depends on the ability to evaluate and act upon performance-related data. Without strong institutionalized feedback mechanisms, access to crucial data for evaluating CDA effectiveness becomes limited.

Operational Outcomes of Security Controls

Determining if CDA has created the desired outcome of securing a network is difficult, but CDA can be associated with improvements in network security indicators like breakout time, mean time to failure (MTTF), and mean time to contain (MTTC). Under the MITRE Framework on cyber resiliency, the success of security controls is judged based on key security functions (identification, protection, detection, response, and recovery). However, a change in these functions, due explicitly to CDA, remains difficult to evaluate. The automated reporting systems of certain software solutions, particularly endpoint security, can help collate quantitative data to assess the outcomes created by CDA.

Absorption Capacity

While CDA interventions may be guided by providing the most objectively high-quality training or powerful cybersecurity solutions, such approaches must also ensure recipients can receive and absorb CDA. To this end, measuring a recipient's pre- and post-hoc readiness and absorption can inform an assessment of operational success. Before delivery of CDA, an assessment of a recipient's infrastructure readiness can ensure the operational success of CDA is maximized on arrival. As one CDA provider stated of the provision of threat intelligence to Ukrainian companies:

> *"I think [threat intelligence] is valuable but it could be more valuable. We want to send them intel, but on the practical level, they need approval, they need to talk to their teams, they need to stand up technology to be able to receive, all during an active war."*

After the delivery of CDA, a continued assessment of absorption can contribute to overall assessments of operational success. A recipient's ability to integrate threat intelligence, its response time to cyber incidents, and its perception of its own success in absorbing CDA can be helpful for assessing CDA after its delivery. However, a post-hoc assessment is not without potential for bias. As another CDA provider argued:

> *"I think Ukraine is always going to want more hardware infrastructure no matter what, they're going to want more aid so likely when they receive a thing and say 'This is useless, man' they're probably not going to be really loud about that, because that might disincentivize other folks from coming in."*

CDA recipients may not provide feedback if they believe negative feedback may lead to less assistance, such as being unable to make use of threat intelligence. Thus, recipient impact perception should not be the sole variable in assessing absorptive capacity but measured in concert with other metrics of *Operational Success*.

Performance Evaluation

Established feedback mechanisms of performance-related data are essential to ascertain whether the targets and objectives of CDA are on track or have been met. This should include institutionalizing outcome reporting for both quantitative data collected through automation and qualitative data. This could include baseline surveys from both providers and recipients recording any challenges or redundancies they are facing, mid-term reviews and evaluations, and progress reports. These feedback mechanisms will help identify which elements of CDA are working and which are not, and thereby improve the overall effectiveness of the assistance provided.

Efficiency

The *Efficiency* pillar determines whether resources are cost-effective, aid is delivered promptly, and operations are conducted smoothly. In any context where threats are urgent and communication is difficult, *Efficiency* is vital for effective CDA. By minimizing delays, ensuring appropriate resource provision, and optimizing processes, CDA can be made more effective for receiving parties. Therefore, the evaluation of *Efficiency* is prioritized within the evaluation framework as part of **Phase 1: Immediate.** The *Efficiency* pillar consists of three components:

- **Economic Efficiency:** Economic efficiency involves optimizing existing resources, such as cybersecurity personnel, training programs, and threat intelligence capabilities. Additionally, conducting cost-benefit analyses helps prioritize investments in cybersecurity measures based on their potential impact on reducing risks and enhancing resilience.
- **Operational Efficiency:** Ensuring appropriate utilization of CDA is essential to meet the specific needs and priorities of recipients. Operational efficiency is represented by how well resources fit the purpose for providing the CDA as well as minimal waste in CDA operations.
- **Timeliness**: This component assesses how quickly requests for assistance are received, processed, and resolved. Prompt responses can more effectively tackle emerging threats.

Strategic Planning

Strategic Planning through prioritizing CDA goals and regular information flows between relevant stakeholders will facilitate scaling the CDA model in alignment with the evolving needs in a conflict. This Strategic Planning pillar is evaluated in **Phase 2: Medium-term** and consists of two components, as described below:

- **Specification and Prioritization of Goals:** Emphasizes the importance of clear, mature, and specific goals in the medium to long term to align and adapt CDA interventions, as required. The discrepancy between process-based and prescribed goals reveals challenges in aligning stakeholder objectives, emphasizing the importance of understanding stakeholders' needs and expectations.
- **Relevant Information Disclosure:** Openness, clarity, and accessibility to relevant information among stakeholders ensures that aid delivery aligns with overarching CDA strategies and commitments, enables a better understanding of recipients' priorities and needs, as well as facilitates effective coordination and accountability within CDA intervention.

Specification and Prioritization of Goals

The specification and prioritization of goals component aims to assess the clarity and alignment of the CDA intervention's objectives. Existing frameworks, such as the MITRE framework and NIST 2.0 CSF, measure security in the context of qualitative or process-based goals (i.e., “support Ukraine’s cybersecurity” as opposed to the outcome-based “reduce Russia-nexus intrusions into Ukrainian systems by 50%”).[23] However, the absence of a concrete method for evaluating security controls often necessitates substituting these with fulfilling organizational goals for CDA. This underscores the urgent need for clear and specific goals in CDA interventions to inform strategic planning.

In interviews with CDA providers, respondents often described their goals for providing CDA as process-based. Goals ranged from the more specific "provide software and hardware, training, intelligence sharing, and strategy advising, and help [Ukraine] avoid mistakes, and shape government approach to cybersecurity" to the vague "help Ukraine resist Russian aggression" to "just continue to help." One provider described their organization's goals as "ambiguous."[24] Coordinators on the ground in Ukraine involved in managing CDA relationships with Ukrainian recipients described the Ukrainian side's goals similarly as "using the resources and experience" of US cybersecurity leaders to "produce strategy."[25] While process-based goals like the ones above are helpful in the short term, especially in situations when quantitative data is unavailable, mature, clear, and specific goals are essential for medium to long-term alignment and scalability of CDA interventions as conflicts evolve.

Under a "help-out" process-based goal like the one described by several providers, CDA in Ukraine to date (providing millions in aid and countless volunteer hours) might be considered a success simply by being a net positive for Ukraine. However, under a different, more prescribed goal, these achievements would be insufficient. The below quote from a CDA coordinator involved in aid distribution describes how efforts have "fallen short" of another larger goal: adequately securing Ukraine in its entirety.

> *"Cybersecurity is dictated by what you can spend...This is part of my frustration: sometimes, people have thrown us a bone of a couple hundred thousand, or maybe we'll get ten million. But hundreds of millions of dollars are required to adequately secure an entire country and provide what's needed. I felt it was almost ridiculous sometimes when we were talking about these minuscule numbers."*

As the two sets of different goals show, an organization providing CDA might consider interventions effective under one set of goals ("help out") but not effective enough under another ("secure an entire country"). This highlights the potential challenges and complexities in aligning different stakeholders' objectives. Internal and external stakeholders may also have different or conflicting goals for their CDA delivery, making it even more difficult to agree on outcomes to target. However, the absence of a concrete method for evaluating security controls often necessitates substituting these with fulfilling organizational goals for CDA. This underscores the urgent need for clear and specific goals in CDA interventions to inform strategic planning. As the conflict progresses, and providers may seek to scale up their CDA intervention in response, ensuring stakeholder involvement and goal alignment is essential to develop strategies to improve the provision and impact of provided security controls, threat intelligence, and training.

The discrepancy between process-based and prescribed goals underscores the importance of specifying and prioritizing goals in CDA interventions to ensure clarity and alignment with broader strategic objectives. Moreover, it measures the understanding and consideration of internal and external stakeholders' needs and expectations in the goal-setting process, which is crucial for fostering collaboration and achieving meaningful outcomes in CDA.

Relevant Information Disclosure

Transparency and accessibility to information related to decision-making processes of providing aid are important elements that facilitate the strategic planning of CDA interventions. This can be evaluated based on the openness of communication channels between a provider and recipient, including providing clear information on strategic planning and commitments; regular information flows on strategic plans and priorities vis-a-vis procurement and allocation of aid, cyber defense strategies, incidents, and outcomes. This will assist in evaluating whether the aid being delivered aligns with the overall CDA strategy and commitments. If the public is identified as one of the stakeholders, transparency can be gauged by assessing whether the organization is committed to reporting challenges, setbacks, and failures consistently and publicly, along with lessons learned.

Disclosure of relevant information should encompass financial and/or budgetary information for relevant stakeholders, including aid that is required, aid that has been delivered (such as software, hardware, training, or services) in numbers, funding sources, and commitments to CDA. Indicators within this component consider the extent to which comprehensive details about the project and activities being undertaken are collated by the provider and shared with recipients and other stakeholders, where applicable. These details include:[26]

- the timelines of CDA (date requested and date delivered)
- details of the recipient that received the assistance
- details of the provider that provided the assistance
- details on the value and type of assistance
- description of the assistance or the name of the license/training/product
- quantity of products or licenses delivered to the recipient
- the current status of the software, hardware, or service that has been delivered (whether in use, not in use, or under training)

Friction

The *Friction* pillar assesses how well CDA providers and recipients respond to the inherent challenges that can hinder the delivery and effectiveness of CDA. This pillar is situated in **Phase 3: Long-term** evaluation, to account for the points of friction that emerge over the course of the war – the "fog of war" as emphasized in interviews with CDA stakeholders.[27] In a wartime environment where information is often incomplete or difficult to access, decision-makers may struggle to identify the specific needs of recipients in conflict zones, due to the novelty of the operation, lack of standard operating procedures (SOPs), time zone differences, and reliance on volunteers, which subsequently can impede or delay decisions around which CDA interventions to prioritize. It is critical to evaluate how a CDA provider and recipient might assess and take steps to mitigate such challenges, given their negative repercussions for progress toward other pillars. The *Friction* pillar is comprised of three components:

- **Historical Presence:** Assesses the importance of relationships and existing connections in conflict zones for the success of CDA interventions. This component evaluates the extent to which early relationship building facilitates rapid aid delivery and prioritizes recipient needs.
- **Logistical Challenges:** Assesses the establishment of standard operating procedures (SOPs) to overcome logistical challenges related to CDA, including time zone differences, technical skill gaps, language barriers, and other intrinsic factors that complicate aid delivery and associated efforts.
- **Risk Identification and Management:** Assesses whether there are processes in place to identify and manage risks faced by both CDA providers and recipients before and during conflict. It includes strategies to address internal risks to a CDA organization and a plan to identify and address external risks. Internal risks may include risk to personnel or operational disruptions, prompting CDA providers to reconsider their involvement or the extent of their involvement to minimize exposure. External risks may arise from operational disruptions, including heightened targeting by adversaries through cyber activity or political attacks.

Sustainability

The *Sustainability* pillar considers the extent to which the net benefits of CDA interventions continue or are likely to continue in the future. CDA interventions should not only provide immediate assistance but also enable recipient organizations to develop lasting capabilities for cyber defense and resilience, even after the withdrawal or reduction of CDA.[28] Therefore, ensuring the sustainability of CDA is critical in building an enabling environment where recipients can independently prevent or respond to cyber incidents, eliminating the need for continuous external assistance. The *Sustainability* pillar is assessed in **Phase 3: Long-term** evaluation, focusing on two key components that address the organizational aspects of CDA:

- **Capacity Enhancements:** Measures the longevity of impacts beyond the intervention, specifically regarding knowledge transfer and the development of organizational capabilities. This includes CDA interventions that seek to equip recipients with the skills and tools necessary for sustained cyber defense readiness, such as training sessions and hands-on support in implementing best practices and technologies that bolster their cyber infrastructure.[29]
- **Post-Intervention Sustainability:** Evaluates the effectiveness of partnerships and collaborative efforts beyond the initial CDA interventions. This component is crucial for integrating strategies into ongoing cybersecurity operations, ensuring policies align with strategic cybersecurity goals. Long-term planning and sustained political support are essential to foster an environment conducive to ongoing cyber resilience. Effective sustainability strategies are vital to ensure that once the direct intervention concludes, recipients are not left vulnerable but are better integrated and equipped to handle future cyber challenges.

Capacity Enhancements

The capacity enhancements component emphasizes the transfer of knowledge and strengthening of organizational capabilities for recipients, including cyber defense infrastructure. In the long term, knowledge sharing empowers recipients to confront present challenges and adapt to emerging threats. Efforts to enhance a recipient's organizational capacity, in concert with knowledge sharing, are essential to ensure the effective application and sustainability of the new competencies and resources. This includes bolstering internal procedures and systems to sustain enhanced cybersecurity measures, enabling recipients to govern their cyber defense strategies autonomously. [30]

Post-Intervention Sustainability

Evaluating post-intervention sustainability seeks to validate whether the CDA intervention has influenced the recipient organization's ability to develop solid partnerships, ensure strategic policy alignment and planning, and adapt to volatility in political commitments and external state contributions.

This component also considers the extent to which organizations have developed a well-structured transition and exit strategy. This strategy should clearly outline a gradual reduction in direct assistance, shifting the focus to enhancing the recipients' capabilities until external support becomes unnecessary. The transition must be seamless, ensuring no loss of operational capability, and should include clear milestones to confirm the recipients' readiness to manage their cyber defense. An effective exit strategy confirms the sustainability of the improvements made and sets a precedent for future CDA initiatives, ensuring that each step contributes towards building a self-reliant cyber defense posture.

Framework Implementation and Recommendations

To implement this framework, CDA stakeholders may adopt one of two approaches:

1. **Self-evaluation:** investigation of its own operations against the framework based on empirical data available only to the CDA provider, recipients, and other stakeholders.
2. **Survey-style evaluation:** providers, partners, and recipients evaluate the organization based on the framework and provided survey questions.

Based on these approaches, the report concludes five key recommendations for the practical implementation of a CDA evaluation framework.

Table 5: Summary of Recommendations

	Recommendation	Timeline	Description
1	***Strengthen mechanisms for accessing data and receiving feedback reports.***	Short Term + Long Term	Reporting is critical to measuring CDA effectiveness; thus, a structured mechanism for ongoing stakeholder feedback regarding the CDA is critical for improving effectiveness.
2	***Operationalize the framework by either performing an in-depth self-evaluation or collecting evaluations from stakeholders.***	Short Term + Long Term	The framework should be disseminated to CDA stakeholders. In the long term, CDA providers should conduct a self-evaluation using the evaluation framework to provide a stronger picture of CDA effectiveness.
3	***Assess indicators with a standard deviation (SD) > 1.5 to identify areas lacking consensus.***	Short Term	When the SD exceeds 1.5 (No consensus), it suggests significant variability in responses possibly due to ambiguous phrasing, language barriers, or differing interpretations.
4	***Include a diverse range of stakeholders in the indicator selection process.***	Short Term + Long Term	The indicator selection process should involve cybersecurity experts, beneficiaries, policymakers, and practitioners. This diverse representation helps mitigate biases and ensures the indicators reflect a wide range of perspectives, thereby enhancing the objectivity of the evaluation framework.
5	***Utilize pilot testing to refine the framework implementation process.***	Short Term	Implement pilot testing of the selected indicators to evaluate their effectiveness and applicability. Establish an update process for the evaluation framework, considering emerging cyber threats, technological changes, and shifts in the geopolitical environment.

Lessons Learned

While building the framework for evaluating the effectiveness of CDA, several key issues emerged that warrant additional highlighting. These additional lessons learned should be held separate from the implementation of the CDA effectiveness framework and considered broader lessons for the success of CDA efforts as a whole. Expert interviews and reviews of existing literature emphasized two key lessons learned:
1) the importance of a "sequenced approach" to CDA and 2) the importance of planning and budgeting for reporting and data collection from the outset of CDA provision.

Towards a Sequenced Approach to CDA

Analysis from the RAND Corporation categorizes military aid regimes into three major approaches of varying efficacy: the "weapons-first" approach, the "overhaul" approach, and the "sequenced" approach. CDA should follow a sequenced approach by prioritizing trust-building with partners, aligning strategic priorities between providers and recipients, and prioritizing the needs of the recipient over the heuristic preferences of the provider.[31] RAND describes the need to communicate with and center the needs of the partner when delivering aid:

> *"Effective institution-building support, when done right, is closely tied to the unique characteristics of the partner rather than driven by what has worked for the U.S. military in its own institutions... Building such an institutional foundation advances the absorptive capacity of the partner force, increasing the likelihood that the partner will employ new capabilities effectively and that any increase in... performance is sustained beyond the timeline of the U.S. mission."*
>
> *- Noyes, Alexander, and Richard Bennet, RAND, Making Military Aid Work*

Rather than flooding a partner country with cybersecurity tools and resources it cannot use, or seeking to rebuild cyber infrastructure in the American or Western image, CDA must take time to build and leverage trusted relationships with recipients and coordinators. As one CDA provider noted:

> *"One of the most important elements that has made us successful, I would say the most important element that has made us successful, is trust. Building personal trust relationships downrange with specific individuals. And I mean specific individuals, not even necessarily organizations."*

The leveraging of cyber relationships established as far back as 2013 has been described as a major factor in the delivery of CDA to Ukraine. However, analysis has suggested that a majority of the groundwork laid for CDA in Ukraine was spurred by Russia's 2014 annexation of Crimea, a period which included frequent and sophisticated cyberattacks.[32] CDA providers must not assume that analogous relationships exist in every future site where CDA is needed. Providers must recognize that additional political will and impetus will be required in the next use case for CDA to build relationships before the onset of a critical cyber threat.

Planning to Collect: Reporting and Data as Critical to Evaluating CDA Effectiveness

CDA requires strong data collection and reporting mechanisms in order to evaluate effectiveness, but this collection cannot always occur on request. Various experts involved in CDA provision to Ukraine have suggested that while it would be valuable to receive data on which forms of aid have been successful, CDA providers cannot reasonably expect or mandate Ukrainian firms to consistently provide feedback while under siege. As one senior cybersecurity executive put it:

> *"Feedback is very important for [assessing impact], but feedback is hard to give in a warzone. I'm not going to sit there and tell people with tanks rolling through their city that they need to sit down and give me feedback about my threat intel. We're able to get some relevant stats back through our tech thanks to automation, we just need to do little analytics on it. However, we also can't always get all their analytics if they're government or military."*

While requesting feedback from recipients may not always be logistically possible or even necessary for the provision of aid a lack of effective reporting can create negative repercussions that CDA organizations must understand and consider.[33] Lack of feedback affects a CDA organization's ability to assess success but also affects its efficiency and transparency by obscuring what resources are being used by recipients.

Reporting can also have positive effects on a CDA organization's sustainability. Sharing compelling evidence of success stories can increase participants' political will to provide CDA, and donors' willingness to provide funding. One CDAC provider recommended that letters of appreciation or other simple documentation acknowledging a provider's contribution would be effective for CDA sustainability as they help sustain trusted relationships and maintain political will.[34] Reporting on such successes would serve as a validation of CDA providers and serve as effective marketing for providers.[35]

For future CDA efforts, consciously budgeting for data collection and reporting in advance of aid delivery is considered the best way to ensure there are mechanisms in place to evaluate the effectiveness of CDA. As one expert involved with foreign aid and cyber capacity building described:

> *"I think having defined objectives and assigned personnel is key [for data collection]. So I think what I recommend is that if we are requiring M&E, monitoring and evaluation for data collection, the expectation is that there is a set program design that doesn't come at the end of the program, but is included at the beginning of the program as part of the program design, as part of the program budget, to allocate x percent of the project to data collection. And that's something that I think is a best practice."*

Owing to the young age of the CDA field, CDA organizations may not have matured to include allocations for data collection in their budgets. However, the most likely reason for any lack of collection capabilities is a lack of consistent funding for the CDA effort as a whole. An evaluation paradox emerges wherein CDA organizations are unable to concretely demonstrate their effectiveness without large amounts of funding, but donors are unwilling to provide said funding because CDA organizations have yet to concretely prove their effectiveness. The interviewed aid expert reiterates:

> *"I want to re-emphasize the fact that in order to collect… there needs to be a budget allocated for dedicated personnel or third-party agency. It needs to be part of the program design. It needs to be part of the contracting paperwork for the implementers. It needs to be a requirement… so I think that there has to be some responsibility and accountability on our end, that we need to go beyond just the intention of assistance. "*

The negative feedback loop between low and inconsistent funding and evaluation difficulties can only be broken by CDA funders, donors, and governments. Without major financial support, CDA providers cannot prove the effect of their CDA.

Conclusion

Assessing the effectiveness of CDA is a critical requirement for improving interventions to meet the challenge of hybrid warfare. The five-pillar framework presents a novel approach to evaluate CDA, structured across three phases to identify successes and shortcomings in enhancing the cyber defenses of nations in conflict.

CDA is an evolving and dynamic field just like the rest of cyberspace, and implementers of the framework should consider it a living document to be updated as understanding of the field grows. Pillars to assess CDA effectiveness may change in weight depending on the scenario, the recipients, and any number of factors. However, evaluators of CDA should take *Operational Success, Efficiency, Strategic Planning, Friction,* and *Sustainability* as a baseline to supplement or subtract from as they see fit, for the specific needs of the conflict they are addressing.

Ultimately, while CDA provision without evaluation is more convenient and less costly, it is a fallacy to suggest that CDA can be provided forever without an understanding of its impacts. All forms of assistance, including CDA, have the potential not just to be ineffective, but to do harm if not distributed effectively and responsibly. However, as profiled in this report, data collection and reporting on the effectiveness of CDA comes at a high financial cost, and donors' support for CDA must rise to meet this requirement.

Future CDA efforts must anticipate needs and many providers already have one eye on the next site for providing assistance: a Taiwan Strait contingency. CDA will be needed to ensure Taiwan's network resiliency is sufficient to withstand attacks from Chinese cyber actors. The framework presented in this report can help evaluate preparedness for a Taiwan scenario and help stakeholders strategize for effective CDA.

In developing the framework, this report sheds light on which preparations will be required and which actions would be most effective during (and more importantly, before) a Taiwan scenario. During peacetime, CDA leaders must build connections and preparedness in Taiwan (and any other site it views as potential sites for the next hybrid war) to follow a sequenced approach to CDA and lay the groundwork for future operations. A CDA model for operations in Taiwan would necessarily require new partners to serve as coordinators and points of contact, and pre-emptively building aid connections in Taiwan can help a CDA replicate the advantage CDAC gained from its pre-existing ties in Ukraine.

CDA, just like cyberspace itself, is built on trust between providers and recipients. Donors and grant funders have a major opportunity moving forward to be a part of building this vital trust in the evolving fields of cybersecurity and assistance provision, and to greatly enhance our collective understanding of how CDA can support a country in crisis. Much of the potential for evaluating this exciting and important field of aid remains constrained by a lack of resources and political will, but supporters of CDA have a unique and exciting opportunity to unlock its potential for cyber capacity building with their future support.

Appendix 1: Evaluation Framework

PILLAR: OPERATIONAL SUCCESS				
Component	**Indicator**	**Description**	**Type**	**Measurement**
Operational Outcomes of Provided Security Controls	Network Security	Measures the change in frequency and severity of cyber incidents or breaches over a specified period, following the implementation of provided security controls.	Direct	Prevalence Data on Number of Cyber Incidents and Breaches
			Proxy	Recipient and Provider Feedback
	Attack Surface Management	Measures the identification, assessment, and reduction of vulnerabilities and exposure within a recipient organization's attack surface.	Direct	Percentage of Attack Surface Reduction through Vulnerability Remediation
				Number of New Attack Vectors Discovered and Mitigated in a Given Period
				Mean Time to Acknowledge (MTTA) Changes to Attack Surface
	DDoS Mitigation	Measures the capability to detect, mitigate, and prevent DDoS attacks.	Direct	Number of DDoS Attacks Mitigated in a Given Period Following Implementation of Provided Tools
				Mean Time to Respond (MTTR) to DDoS Attacks
	Endpoint Security	Measures the impact of provided tools on protecting individual devices (endpoints).	Direct	Number of Detected Threats (Malware, Ransomware, Phishing Attacks) Detected and Blocked by Provided Endpoint Security Solutions over a Given Period
				Dwell Time
			Proxy	Recipient Feedback
Absorption Capacity	Incident Response Time	Measures reduction in incident response time over a given period.	Direct	KPIs for Incident Response Management including Mean Time to Respond (MTTR)
			Proxy	Recipient Feedback
	Threat Intelligence Integration	Measures the relevance of provided threat intelligence to the recipient’s environment.	Proxy	Recipient Feedback
	Infrastructure Readiness	Assesses whether the CDA organization has the necessary physical and technological infrastructure to facilitate aid delivery.	Proxy	Provider and Recipient Feedback
	Recipient Impact Perception	Measures recipient perception of the impact of provided CDA on overall defense.	Proxy	Recipient Feedback
Performance Evaluation	Feedback Mechanisms	Assesses mechanism to facilitate open exchange of feedback and data between the provider and recipient.	Proxy	Recipient Feedback

PILLAR: EFFICIENCY

Component	Indicator	Description	Type	Measurement
Economic Efficiency	Cost-Effectiveness	Assesses the cost-effectiveness of financial and resource contributions by the provider.	Direct	Financial Statements
			Proxy	Provider and Recipient Feedback
Operational Efficiency	Resource Utilization: Security Controls	Measures the utility of cybersecurity solutions provided to the recipient, identifying instances of under-utilization and over-utilization.	Proxy	Provider and Recipient Feedback
	Resource Utilization: Threat Intelligence	Measures the utility of threat intelligence provided to the recipient, identifying instances of under-utilization and over-utilization.	Proxy	Provider and Recipient Feedback
	Resource Utilization: Training	Measures the utility of training provided to the recipient, identifying instances of under-utilization and over-utilization.	Direct	Training Participation Rates
			Proxy	Provider and Recipient Feedback
Timeliness	Timeliness of Request Fulfillment	Measures both the number of requests fulfilled, and the time taken from request to fulfillment. the speed of the CDA organization in fulfilling requests for assistance.	Direct	Number of Requests in a given Period
				Time from Request to Fulfillment
			Proxy	Provider and Recipient Feedback

PILLAR: STRATEGIC PLANNING

Component	Indicator	Description	Type	Measurement
Specification and Prioritization of Goals	Goal Alignment	Measures the extent of clarity in goal specification and alignment of the CDA intervention.	Proxy	Provider and Recipient Feedback
	Stakeholder Engagement	Measures the extent to which stakeholders' needs and expectations are considered in the goal-setting process.	Proxy	Provider and Recipient Feedback
Relevant Information Disclosure	Disclosure of Organizational Information	Assesses the availability of organizational information, operational data, and cyber defense strategies to CDA providers and recipients.	Proxy	Provider and Recipient Feedback
	Disclosure of Cyber Incidents and Threats	Assesses the extent to which data on cyber incidents and threats are shared between CDA providers and recipients.	Direct	Data on Cyber Incidents from Providers and Recipients
			Proxy	Provider and Recipient Feedback
	Disclosure of Financial and Logistical Assistance	Assesses the extent and quality of disclosure regarding financial and logistical support provided to and by entities involved. the availability of economic and budget information to CDA providers and recipients.	Direct	Number of CDA Providers
				Expenditure Reporting
			Proxy	Provider and Recipient Feedback
	Disclosure of Partnerships	Assesses the availability of information on the provider's partnerships and collaborations, with other organizations, governments, or private entities, that may impact (positively or negatively) aid provision.	Direct	Official Documents and Statements
		Assesses the availability of information on the provider's partnerships and collaborations, with other organizations, governments, or private entities, that may impact (positively or negatively) aid provision.	Proxy	Provider and Recipient Feedback

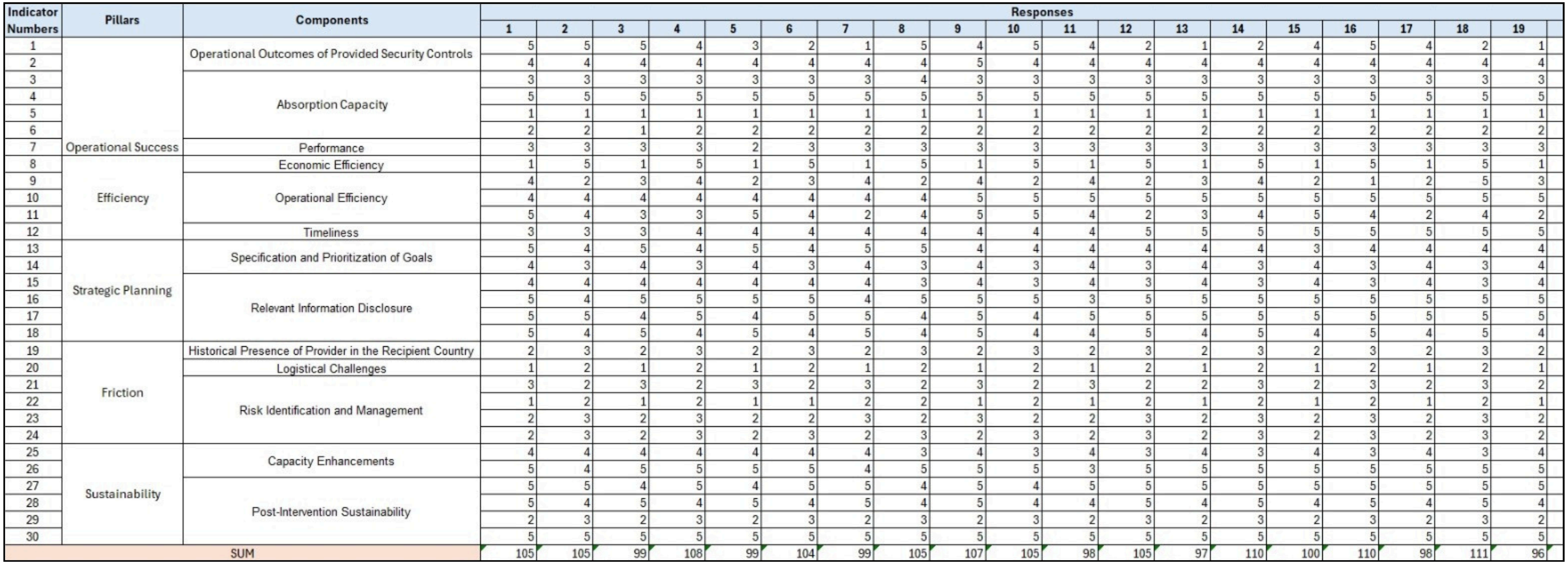
PILLAR: FRICTION

Component	Indicator	Description	Type	Measurement
Historical Presence of Provider in the Recipient Country	Duration of Relationship between Provider and Recipient	Assesses the relationship between the CDA organization and recipient before initiating CDA.	Direct	Financial Data on Historical Assistance Value to Recipient from Provider
				Case Studies
			Proxy	Provider and Recipient Feedback
Logistical Challenges	Gaps between People, Processes, and Technology that Create Challenges for CDA Provision	Assesses whether the organization has strategies in place to tackle logistical challenges to streamline aid delivery.	Direct	Number of Strategic Plans Specifically Addressing Logistical Challenges
				Time Reduction in CDA Delivery Due to Implemented Strategies
			Proxy	Provider and Recipient Feedback
Risk Identification and Management	Risk Management Objectives	Assesses the establishment and alignment of risk management objectives between providers and recipients.	Proxy	Provider and Recipient Feedback
	Risk Appetite and Tolerance	Assesses communication of risk appetite and tolerance statements between the provider and recipient.	Proxy	Provider and Recipient Feedback
	Communication and Documentation of Risk	Assesses the extent of established communication channels between providers and recipient organizations to communicate risk.	Direct	Assessment of Standard Operating Processes (SOPs)
			Proxy	Provider and Recipient Feedback
	Risk Mitigation	Measures the extent to which risk mitigation strategies have been established and implemented by providers and recipients.	Direct	Strategy Documents
			Proxy	Provider and Recipient Feedback
	Vulnerability Management	Measures the level of vulnerability management practices in place to identify and mitigate risks.	Direct	Vulnerability Remediation Time
				Patch Coverage (% of Known Vulnerabilities that have been Patched within a Specific Timeframe)
				Incident Response Metrics (MTTD and MTTR)

PILLAR: SUSTAINABILITY				
Component	**Indicator**	**Description**	**Type**	**Measurement**
Capacity Enhancements	Knowledge Transfer	Assesses the extent of knowledge transfer between provider and recipient.	Proxy	Recipient Feedback
	Organizational Capability Enhancement	Assess enhancements in organizational capabilities and practices related to cybersecurity governance, risk management, and compliance because of CDA provision.	Direct	Percentage of Recipient Organizations with Documented Cybersecurity Policies and Procedures
			Proxy	Recipient Feedback
Post-Intervention Sustainability	Partnerships and Collaboration	Assess how partnerships established during CDA interventions can ensure the sustainability of cybersecurity enhancements.	Direct	Number of Memorandums of Understanding (MOUs) between Provider and Recipient Organizations
			Proxy	Provider and Recipient Feedback
	Policy Alignment	Assesses how CDA interventions have influenced the alignment of national or organizational cybersecurity policies, strategies, and regulations with international standards.	Direct	Official Statements and Strategy Documents
			Proxy	Provider and Recipient Feedback
	Long-term Strategic Planning	Assess the projected assistance timeline and resource provision of the provider, including planning for reducing or withdrawing CDA.	Direct	Number of Security Controls Donated (licenses etc.)
				Contractual documents between Provider(s) and Recipient(s)
			Proxy	Provider and Recipient Feedback
	Political Will	Assesses factors influencing long-term political engagement on the part of the provider, and recipients.	Direct	Official Documents and Statements by Governments and Organizations
			Proxy	Provider and Recipient Feedback

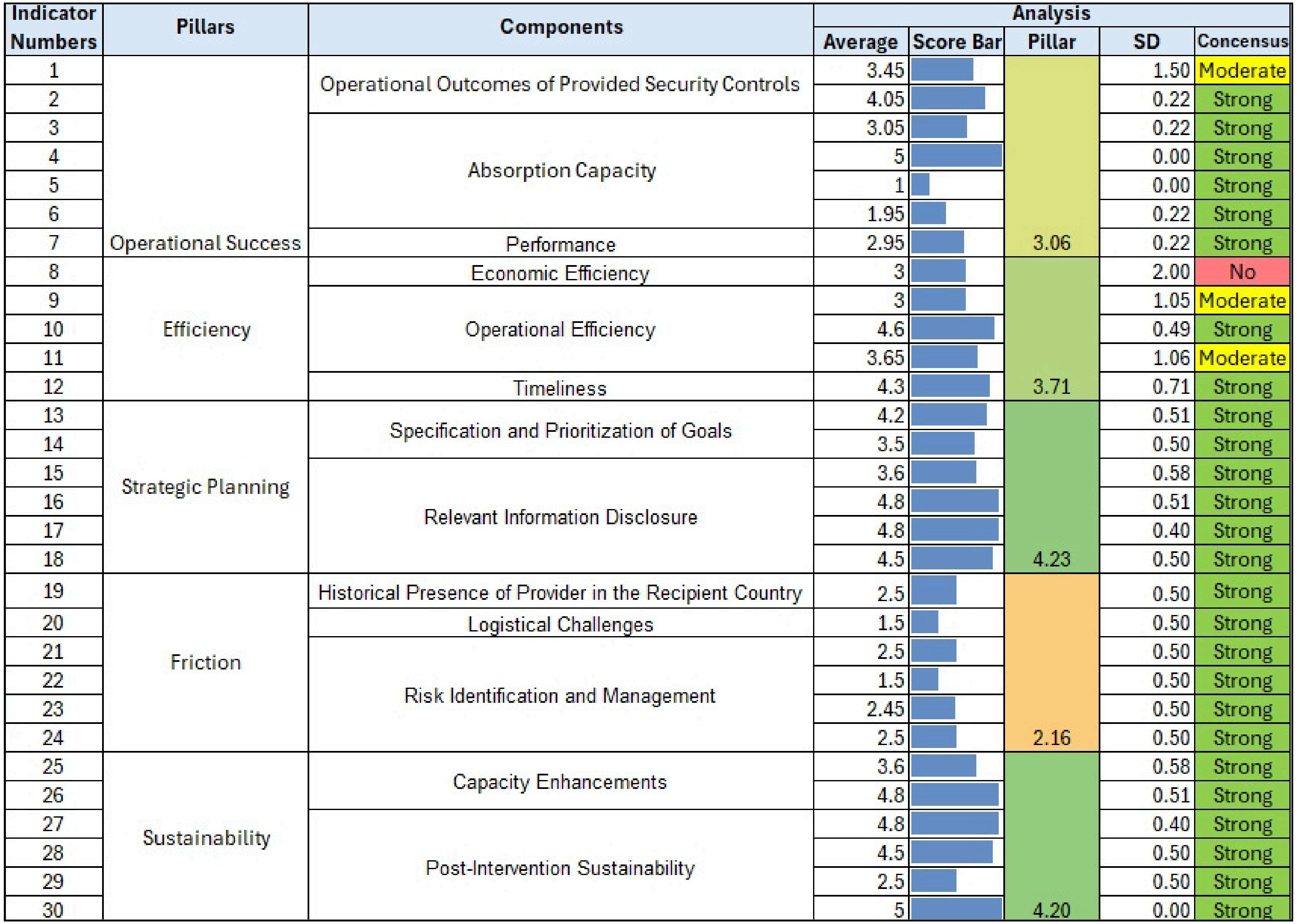
Appendix 2: Proxy Indicator Analysis and Visualization

Image 1: Sample Collection of Proxy Indicator Responses



Indicator Numbers	Pillars	Components	Responses																		
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	Operational Success	Operational Outcomes of Provided Security Controls	5	5	5	4	3	2	1	5	4	5	4	2	1	2	4	5	4	2	1
2			4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4
3		Absorption Capacity	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3
4			5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
5			1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6			2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
7		Performance	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
8	Efficiency	Economic Efficiency	1	5	1	5	1	5	1	5	1	5	1	5	1	5	1	5	1	5	1
9		Operational Efficiency	4	2	3	4	2	3	4	2	4	2	4	2	3	4	2	1	2	5	3
10			4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	5	5
11			5	4	3	3	5	4	2	4	5	5	4	2	3	4	5	4	2	4	2
12		Timeliness	3	3	3	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5
13	Strategic Planning	Specification and Prioritization of Goals	5	4	5	4	5	4	5	5	4	4	4	4	4	4	3	4	4	4	4
14			4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4
15		Relevant Information Disclosure	4	4	4	4	4	4	4	3	4	3	4	3	4	3	4	3	4	3	4
16			5	4	5	5	5	5	4	5	5	5	3	5	5	5	5	5	5	5	5
17			5	5	4	5	4	5	5	4	5	4	5	5	5	5	5	5	5	5	5
18			5	4	5	4	5	4	5	4	5	4	4	5	4	5	4	5	4	5	4
19	Friction	Historical Presence of Provider in the Recipient Country	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2
20		Logistical Challenges	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
21		Risk Identification and Management	3	2	3	2	3	2	3	2	3	2	3	2	2	3	2	3	2	3	2
22			1	2	1	2	1	1	2	2	1	2	1	2	1	2	1	2	1	2	1
23			2	3	2	3	2	2	3	2	3	2	2	3	2	3	2	3	2	3	2
24			2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2
25	Sustainability	Capacity Enhancements	4	4	4	4	4	4	4	3	4	3	4	3	4	3	4	3	4	3	4
26			5	4	5	5	5	5	4	5	5	5	3	5	5	5	5	5	5	5	5
27		Post-Intervention Sustainability	5	5	4	5	4	5	5	4	5	4	5	5	5	5	5	5	5	5	5
28			5	4	5	4	5	4	5	4	5	4	4	5	4	5	4	5	4	5	4
29			2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2
30			5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
SUM			105	105	99	108	99	104	99	105	107	105	98	105	97	110	100	110	98	111	96

Image 2: Sample Analysis of Proxy Indicator Responses



Indicator Numbers	Pillars	Components	Analysis				
			Average	Score Bar	Pillar	SD	Concensus
1	Operational Success	Operational Outcomes of Provided Security Controls	3.45		3.06	1.50	Moderate
2			4.05			0.22	Strong
3		Absorption Capacity	3.05			0.22	Strong
4			5			0.00	Strong
5			1			0.00	Strong
6			1.95			0.22	Strong
7		Performance	2.95			0.22	Strong
8	Efficiency	Economic Efficiency	3		3.71	2.00	No
9		Operational Efficiency	3			1.05	Moderate
10			4.6			0.49	Strong
11			3.65			1.06	Moderate
12		Timeliness	4.3			0.71	Strong
13	Strategic Planning	Specification and Prioritization of Goals	4.2		4.23	0.51	Strong
14			3.5			0.50	Strong
15		Relevant Information Disclosure	3.6			0.58	Strong
16			4.8			0.51	Strong
17			4.8			0.40	Strong
18			4.5			0.50	Strong
19	Friction	Historical Presence of Provider in the Recipient Country	2.5		2.16	0.50	Strong
20		Logistical Challenges	1.5			0.50	Strong
21		Risk Identification and Management	2.5			0.50	Strong
22			1.5			0.50	Strong
23			2.45			0.50	Strong
24			2.5			0.50	Strong
25	Sustainability	Capacity Enhancements	3.6		4.20	0.58	Strong
26			4.8			0.51	Strong
27		Post-Intervention Sustainability	4.8			0.40	Strong
28			4.5			0.50	Strong
29			2.5			0.50	Strong
30			5			0.00	Strong

References

[1] Cyber Defense Assistance Collaborative Blue Force Tracker, 2024.

[2] Tidy, Joe. BBC News. Ukraine says it is fighting first “hybrid war” https://www.bbc.com/news/technology-60622977

[3] Fortinet Blog. The Increasing Wiper Malware Threat. https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

[4] Ibid

[5] Cyber Peace Institute. “Case Study: Viasat" https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

[6] Newsweek. Ukraine Official Asks Elon Musk for Starlink Stations Amid Russian Invasion. https://www.newsweek.com/ukraine-official-asks-elon-musk-starlink-stations-amid-russian-invasion-1682977

[7]The Record. Russian hackers infiltrated Ukrainian telecom giant months before cyberattack. https://therecord.media/russians-infiltrated-kyivstar-months-before

[8] The Record. Ukraine's cyberattacks on Russia aiding ground operations, top Kyiv cyber official says https://therecord.media/ukraine-cyberattacks-aiding-ground-war-russia

[9] Rattray, Greg, et al. The Cyber Defense Assistance Imperative Lessons From Ukraine, Feb. 2023, www.aspeninstitute.org/wp-content/uploads/2023/02/Aspen-Digital_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf

[10]Cyber Defense Assistance Collaborative (CDAC). (2023). BFT Convening November 2023: Overview of Assistance and Strategy.

[11]Noyes, Alexander, and Richard Bennet. RAND. Making Military Aid Work https://www.rand.org/pubs/commentary/2023/07/making-military-aid-work.html

[12] Stabilization Assistance Review: A Framework for Maximizing The Effectiveness of US Govt Efforts to Stabilize Conflict Affected Areas www.state.gov/reports/stabilization-assistance-review-a-framework-for-maximizing-the-effectiveness-of-u-s-government-efforts-to-stabilize-conflict-affected-areas-2018/

[13] OECD. “Applying Evaluation Criteria Thoughtfully.” https://doi.org/10.1787/543e84ed-en

[14] Bodeau, Deborah J., et al. MITRE, 2018, Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods, https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

[15] Cadot, Olivier, et al. USAID, Where to Spend the Next Million? Applying Impact Evaluation to Trade Assistance. https://www.usaid.gov/sites/default/files/2022-05/Next-Million.pdf

[16] NIST. National Institute of Standards and Technology Framework (2.0) https://doi.org/10.6028/NIST.CSWP.29

[17] Interviews Conducted from February 16, 2024 to April 5, 2024

[18] See Appendix 1 for the full table.

[[19] Kaplan, James, and Jim Boehm. “The Pitfalls in Measuring Cybersecurity Performance,” May 9, 2017. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-blog/the-pitfalls-in-measuring-cybersecurity-performance.

[20] See Image 1 in Appendix 2 for Rating Scale Descriptions and Evaluation.

[21] Christensen, Larry B. Research Methods, Design, and Analysis. PRENTICE HALL, 2022.

[22] Should any indicator exhibit a standard deviation above 1.5, further actions—such as follow-ups with respondents—are advised to clarify potential ambiguities and ensure the reliability of the framework's findings. See Image 2 in Appendix 2 for Survey Responses and Analysis Summary.

[23] Bodeau, Deborah J., et al. MITRE, 2018, Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods ; NIST. National Institute of Standards and Technology Framework (2.0)

[24] Interviews Conducted February 23 and March 11, 2024.

[25] Interview Conducted February 22, 2024

[26] Cyber Defense Assistance Collaborative (CDAC), Blue Force Tracker, 2023.

[27] Interviews Conducted from February 16, 2024 to April 5, 2024

[28] OECD. “Applying Evaluation Criteria Thoughtfully.” https://doi.org/10.1787/543e84ed-en

[29] Interview Conducted February 16, 2024

[30] Interview Conducted February 22, 2024

[31] Noyes, Alexander, and Richard Bennet. RAND.Making Military Aid Work www.rand.org/pubs/commentary/2023/07/making-military-aid-work.html

[32] Brooks, Mary. “What America Learned from Cyber War in Ukraine—Before the First Shots Were Fired.” Wilson Center, https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/FINAL%2024-050_Cyber-Ukraine.pdf

[33] Interview Conducted February 16, 2024

[34] Interview Conducted March 8, 2024

[35] Macaes, B. Time. How Palantir Is Shaping the Future of Warfare. https://time.com/6293398/palantir-future-of-warfare-ukraine/

COLUMBIA | SIPA
School of International and Public Affairs

CDAC
A CRDF GLOBAL INITIATIVE