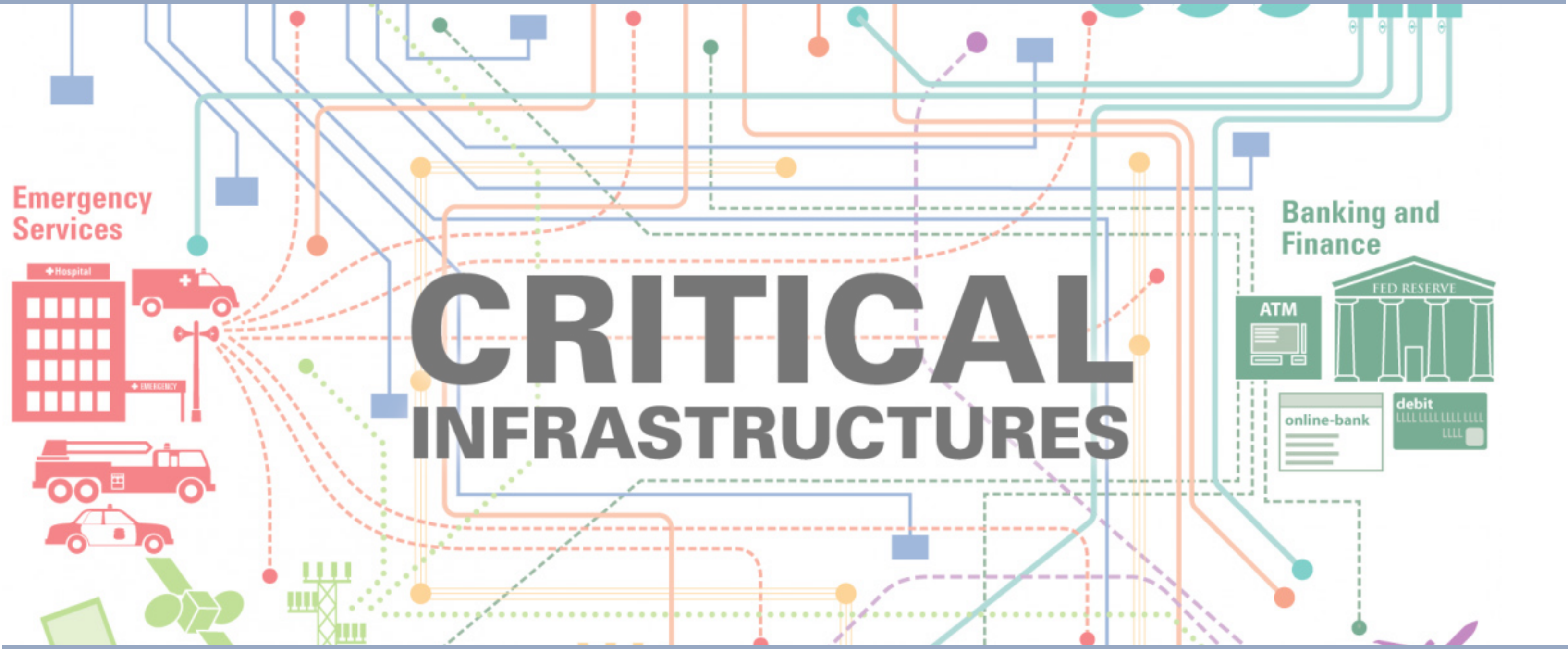
Building Critical Infrastructure Communities

Agreement Number: W911NF-20-S-0008
Award Period: November 1, 2023 - September 30, 2024
Reporting Period: November 1, 2023 - September 30, 2024

FINAL REPORT



TRENDS GLOBAL

SherpaWerx

TEAM

SHERPAWERX:

Paul Wertz

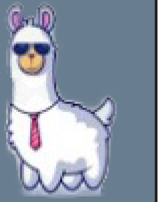
TRENDS GLOBAL

Volker Franke
Anne Chance
Graham Gintz
Amanda Guidero
Lina Tuschling
Timo Zwarg

For more information please contact the project directors:
Volker Franke: volker@trendsglobal.org
Paul Wertz: paul@sherpawerx.com

Disclaimer:
The views expressed in this publication do not necessarily reflect the views of the Army Cyber Institute(ACI), the United States Military Academy at West Point, or the United States Government.

TABLE OF CONTENTS



Abbreviations

Abbreviations

AFCEA - Shortened from Armed Forces Communications & Electronics Association

ACI - Army Cyber Insitute

C-CIC - Cyber Critical Infrastructure Community

GEMA - Georgia Emergency Management and Homeland Security Agency

Acknowledgments

We would like to thank the Army Cyber Institute (ACI) for supporting this project and the cybersecurity community members who offered their expertise and knowledge in support of the development of this project. Their input has been invaluable to shaping the critical infrastructure Portal. We are also grateful to the early adopters of the Portal for their membership and contribution to building this community.

Executive Summary

With funding from the Army Cyber Institute, SherpaWerx and TRENDS Global explore how to strengthen and grow virtual communities to support individuals and organizations involved with protecting and securing civilian critical infrastructure through virtual engagement. This project facilitates the development of an intentional Cyber Critical Infrastructure Community (C-CIC) for the metro Atlanta area to strengthen communication between key partners and strengthen the resilience of said civilian critical infrastructure.

Project Description: The C-CIC project developed and pilot-tested an online Portal to virtually host the Atlanta cyber community and facilitate cross-sector communication and collaboration, which can also support Jack Voltaic-inspired and other readiness workshops, and provide controlled and private spaces to hold sector, interest- and cyber-specific discussions.

Process Overview and Description: The process for designing and implementing the C-CIC Portal, described in detail below, leveraged TRENDS Global's approach to facilitating local engagement to create a community space informed by their needs in a systematic and research-informed process, including the following:

- **Benchmarking.** To prepare for the Portal design for community engagement, the project team benchmarked nine existing online engagement platforms. The results and the accompanying literature review support our operating assumption that the C-CIC Portal is unique in its focus on a specific community and location (local cyber stakeholders in the Atlanta metro Area). Moreover, through customization, the C-CIC Portal is responsive to community needs/wants. It also allowed moderators to create an engagement plan with community members both online and in person to promote and lay the groundwork for sustaining the online community.
- **Visioning and common understanding.**From the literature review and previous experience in community-building projects, we developed a theoretical model that includes five key community-building components: 1) continuous feedback to better understand and respond to community needs, 2) developing a collaborative vision with stakeholders, 3) facilitating shared interest groups, initiatives, and projects, 4) create an opportunity for continuous learning and expertise sharing, and 5) encouraging regular and especially in-person interactions.
- **Adaptation.** To identify areas for improvement in the Portal, we conducted eight interviews with Atlanta-based cyber professionals and members of the Army Cyber Consortium involved in critical infrastructure roles in order to gauge where

members of the critical infrastructure community get information so we can connect the Portal to a growing range of industry resources.

- **Collaborative Capacity.** In addition to expert interviews, we also collected information concerning current coordination efforts for and perceived needs regarding critical infrastructure protection in metro Atlanta through an online survey. The survey offered an initial sense of where coordination could be improved, how to identify additional stakeholders who should be part of our coordination efforts, and how to recruit Portal members. The results indicate strong interest in: 1) community engagement and connections, 2) standardized protocols with better monitoring and response to threats, 3) timely and transparent information sharing, and 4) the need for better access to education and training about risks. The C-CIC Portal offers a locally lead effort to identify and address key concerns within each cyber community interested in adopting the Portal.

- **Community Engagement.** As the final step in the Portal development and community engagement process, we invited community members representing a broad range of institutions/organizations to explore the Portal and share feedback. We conducted four review sessions with eight Beta testers. The Beta testers were generally enthusiastic about potential applications of the Portal. Several observed that the Portal would be a different and new way to share information in Georgia across sectors and agencies. They also provided helpful feedback on the design and functionality of the Portal and the information therein.

- **Resilience and Sustainability.** The project demonstrated the utility and benefits of establishing a virtual Cyber Critical Infrastructure Community. However, the sustainability of any community depends on local support and ownership. While the research that informed this report was made possible through external funding, in the next C-CIC phase, it will be imperative to develop internal funding mechanisms (e.g., through membership fees or sponsorships) to sustain the community.

Deliverable Cyber Critical Infrastructure Community (C-CIC) Web-based Online Community: The result of the work associated with this project is a functional online community engagement platform that is currently being explored by members of the Atlanta critical infrastructure community. Members have access to all resources available for the entire group as well as the ability to establish controlled and private spaces for groups that are only accessible to those who are invited. These subgroups are moderated by the community members themselves.

Next Steps and Future Applications: As the C-CIC Portal continues to be taken up by Atlanta-based critical infrastructure community members, we will continue to

seek additional funding to promote, grow, and sustain the community. Additionally, given the progress in the portal, there is potential to adapt the Portal for use with a number of other communities and special interest groups, such as schools and universities, rural areas, small businesses, and nonprofits that often lack access to state-of-the-art cyber resilience.

Project Description

With funding from the Army Cyber Institute, SherpaWerx, and TRENDS Global explore how to strengthen and grow communities to support those involved with the protection and security of civilian critical infrastructure through virtual engagement. This project assesses critical security needs, existing capacities, interdependencies, resilience, impact of disruptions, and overall protection of these critical resources. Specifically, the project facilitates the development of an intentional Cyber Critical Infrastructure Community (C-CIC) for the metro Atlanta area.

This project allows the Atlanta-based critical infrastructure community to build relationships and rapport in a secure online Portal to ensure more efficient response times and facilitate 24-hour access to comprehensive information, community networks, and threat response mechanisms. The goal is to strengthen existing relationships, networks, and processes and vest key local stakeholders in the virtual community-building process and its outcomes to promote sustainability beyond the project funding phase. The Atlanta C-CIC serves as a pilot for developing and testing a process for Critical Infrastructure Community-building that can be adopted by other municipalities, counties, and states, with the potential to feed into a nation-wide Critical Infrastructure Protection Network.

Process Overview

The process of bringing together metro-Atlanta-based cybersecurity professionals and engaging them in the development of an online community (available via web browser and smartphone apps) involved multiple components, including:

- Developing a project plan and timeline (see APPENDIX A for the C-CIC timeline).
- Scoping the technology to support the community.
- Reviewing the literature on online community building, including communities of practice, to identify best practices for designing and engaging an online community with a focus on sustainability (see Appendix B).
- Benchmarking existing online communities to determine how the C-CIC Portal can improve on currently available levels of engagement from other platform providers while attracting a broader range of cyber security actors than existing platforms, without duplicating their efforts..
- Interviewing members of the cybersecurity community to learn about gaps in communication and needs of the community, identified through peer recommendations.
- Creating a sitemap of the C-CIC Portal to document revisions and propose updates.
- Surveying cybersecurity professionals in the Atlanta metro area to identify opportunities for strengthening coordination among and collaboration between Atlanta-area professionals and potential members of the Critical Sherpas community.
- Inviting beta users to test the Portal and share in-the-moment feedback on the functionality and design of the Portal.
- Adapting what we learned to improve the design and content of the C-CIC Portal and deliver a beta version ready for scale-up and adoption beyond Atlanta and the current performance period.

Process and Results

This section presents more detailed information on the steps within the C-CIC building process and the outputs/outcomes of each step. Building a community in a digital space involves unique challenges that differ from recruiting for and facilitating in-person interactions. Trust and a sense of belonging can develop over time through shared experiences, opportunities, successes, and failures, despite the relative anonymity of online platforms.

Background research and initial Portal design: To prepare for the Portal structure and design, and community engagement, the project team benchmarked nine existing online engagement platforms, including LinkedIn, Digital Community of Peacebuilding Practice, ConnexUs, Platform 4 Dialogue, Cyber Security Insiders, IEEE Cybersecurity Community, ISACA Engage, and collaboration channels including Slack and Discord to identify what services and resources they offer and the cadence of updates and communication. Conflict resolution and peacebuilding sites were included as cybersecurity is inherently about conflict prevention and responsiveness. Using established peacebuilding concepts and practices as a model to develop trust can limit or eliminate conflict during crises. The comparative platform review indicated that many online community-building tools exist to facilitate professional connections and resource sharing. However, most are not targeting specific geographic locations and are more globally oriented. It is hard to assess if they are effective or the extent to which they are utilized by non-members. Many communities of practice sites (predominantly conflict resolution and/or peacebuilding) have outdated, no or few resources. Many cybersecurity communities exist and they likely compete with each other both within and outside of LinkedIn (which, of the sites reviewed, has most groups dedicated to cybersecurity professionals) but are not customizable and are available only to LinkedIn members. Other platforms like Slack and Discord exist mostly to facilitate discussions, not offer additional content such as information or resources. Based on this review, we identified an opportunity to develop a new platform with a local focus able to meet the needs/wants of the professionals themselves rather than using a one-size-fits-all approach that merely leverages the social capital of local members.

In addition to comparing online platforms, we reviewed the literature on online community engagement, paying specific attention to lessons learned, guidelines for success, and discussions of and recommendations for how to avoid common pitfalls. Based on the literature review, we define “online community” as any virtual space where people come together with others to converse, exchange information or resources, learn, play, or just be with each other. The term applies to many social configurations, from small close-knit groups to sites with millions of participants. Online communities may be supported by various technology platforms, from email lists to forums, blogs, wikis, and networking sites. What they all have in common is that they facilitate ongoing interactions among people over time, with some of the interactions being technology-mediated. Validating our understanding of online community building and stakeholder engagement helped us create a successful platform (see Appendix B for literature review).

The results of our benchmarking and the literature review support our operating assumption that the C-CIC Portal is unique in its focus on a specific community and location (local cyber stakeholders in the Atlanta metro Area). Moreover, through customization, the C-CIC Portal is responsive to community needs/wants. It also allowed moderators to create an engagement plan with community members both online and in person to promote the online community. For instance, the literature helped identify steps to building an online community and distinguishing different types of community participation to set realistic expectations in terms of the level of engagement within the community. The best practices derived from the literature are reflected in the Theoretical Model for Community Engagement detailed below.

The portal was engineered to be a scalable platform designed for flexibility conducive to building hybrid communities. Hybrid in this case meaning supportive of both in-person community building events and fully remote community building events with a plan to scale from a few members to hundreds of thousands interacting as needed. The portal was also designed with additional functionality to support groups looking to extend the atmosphere of a conference or training exercises into a lively community dynamic. This includes live streaming capabilities to be inclusive of remote stakeholders as well as in-person guests who have the ability to participate in live training and exercises via live polls. By engineering a scalable portal to allow for both remote and in-person participation, the community portal can best serve in its mission to build an expansive specialized community with customizable spaces of sub-groups who may wish to focus on specific topics or initiatives via desktop computer or in a separate mobile app experience.

Digital community building: Theoretical model

The C-CIC project aimed to cultivate a dynamic and cohesive community of cybersecurity professionals in the Atlanta metro area, fostering authentic communication, information sharing, and collaboration to increase the resilience of critical infrastructure. For this community to be sustainable and continue to grow, a strong sense of belonging is criti-cal. The C-CIC Portal builds belonging through five key community-building components:

1. Continuous Feedback and Understanding Community Needs
2. Communities continuously evolve based on member feedback. The C-CIC Portal is designed to identify and address member interests, opportunities, challenges and needs.

3. We used surveys and discussion threads to gather insights and guide the development of self-identified targeted issue groups and initiatives.
4. Developing a Collaborative Vision
5. Through virtual workshops and brainstorming sessions, the process facilitates the generation of content by community members and builds trust and collaborative resilience by facilitating hope, solutions, and joint projects.

Facilitating Issue groups, Initiatives, and Projects
Members are encouraged to form issue groups based on shared interests. The C-CIC Portal supports the creation and joining of these groups and the facilitation of collaboration across issue groups.

Mentoring, Knowledge Sharing, and Education
The C-CIC Portal offers a forum for continuous learning and expertise sharing, including regular live panels, webinars, workshops, and "ask me anything" sessions with industry experts. Additionally, we set up an expandable resource library of cybersecurity materials.

Locality and In-Person Interaction
We encourage virtual and in-person local meetups and networking events by providing a dedicated space for event announcements, planning and recap. Since the locality and in-person interactions are important means for gaining traction on a local level, this component will be central to the further maturation of the project in which we integrate and combine existing in-person facilitation into our approach.

Needs assessment and key stakeholder input:
To identify areas for improvement in the Portal, we conducted eight interviews with Atlanta-based cyber professionals and members of the Army Cyber Institute Consortium involved in critical infrastructure roles (see APPENDIX C for a list of interviewees and the interview schedule). The goal of the interviews was to gauge where members of the critical infrastructure community get information so we could connect the Portal to a broad range of industry resources, creating a unique repository of cyber information. We also inquired about best practices, opportunities for an online community platform, and suggestions for additional people to invite to participate.

The results of the interviews allowed us to identify key sources of information we used to build the content of the Portal, including posting events, job openings and key websites and news sources. Our interviews also revealed the following gaps in information, technological capacity, communication, and connectivity that the Portal could fill:

- Vendor recommendations/sourcing to identify reliable and security cybersecurity providers.

- Single source or repository that incorporates data feeds from all the key players regarding cyber threats and opportunities, e.g., CISA Resources, Mitre – FFRDC, Linked In, FBI, and News outlets.

- Unified resources for wargame design and development research.

- Events: Other social engagement platforms cannot often effectively host and/or raise awareness for events. Social meeting platforms such as TEAMS or SLACK typically lack common event calendars.

- From a response to disaster/incursion standpoint – how is the cascading impact determined, ie., what is the supply chain, who should we look at downstream, where might threat actors come from and could they have wormed their way in.

- Vetting tools and software to identify reliable and best-in-class tools.

- As one of our interviewees commented: There need to be discussions of risks and problems which should be but are not taking place, "cascading impact, water supply folks need to understand that no water moves unless there is electricity, how long can generators run, gas may not move without electricity – having 24/7 list of contacts, knowing each other, turns on personal relationships – do the gas folks know who their counterparts are in the other CIC?" This is a gap that a portal could fill.

- Best practices for vetting junior staff, interns, project partners, and members.

- The benefit to building the community: if an incursion happens there could be a list in the Portal that they can contact for specializing in legal, GBI, policy, staffing.

- Currently, there is a missed opportunity for collaboration as each CSA doesn't often engage with their counterpart in other segments of the infrastructure, a portal of this nature could connect them.

- Calendar: Other social media platforms like Teams are clunky for the calendar and bring in a common calendar to show events that are going to be happening (common calendar). Need community discussions on the calendar. It would be nice to have one place to go to to populate your calendar.

- Currently, it is hard to locate geographic information. It would be helpful to have information about what critical infrastructure is located where and who do totalk to. This could be managed in the controlled environment of the portal and available only to specific invited members of a specific space.

- A central location to give the Industry familiarity with risk management tech, management, legal, and the resources center of the portal could be categorized to address these and others recommended by members.

Process and Results

Consortium Member Interviews: Areas of Potential Synchronicity

David Schwartz, Rochester Institute of Technology:This highlights the goal of our project, connecting those in the cyber critical infrastructure community, so they know who they need to know. Our Portal is a perfect medium to conduct gaming exercises and we are currently collaborating to take a study about bringing the Rochester Institute of Technology Jack Voltaic into at least one community – to learn more about community engagement.

James Dempsey, Stanford University: Jim mentioned that there is a gap for people on the base, they don't have insight into the cyber resilience of the cic providers on which they are dependent. He sees a need for evolving CS structures at the national level and relationship to what is happening at the community level. Though Jim perceived the Portal as an aggregator, the connectivity potential of the Portal could reduce the gap he mentions.

Scott Shackelford, Indiana University: The obvious area of synchronicity is that we can provide a link to their education and workshops through our Portal. Less obvious, but equally important is that the metro Atlanta area is a great testing ground for a beta group out of the municipality for testing, they would really appreciate that and both we and they could evaluate the efficacy of their program and our Portal.

Kristen Pederson, Norwich University Applied Research Institutes (NUARI): Our area of synchronicity with Kristen and what she does is that cybersecurity is about people and human behavior, not just IT

If you need to know
who you need to know
when you need to know,
you've already lost.
----David Schwartz----

Survey

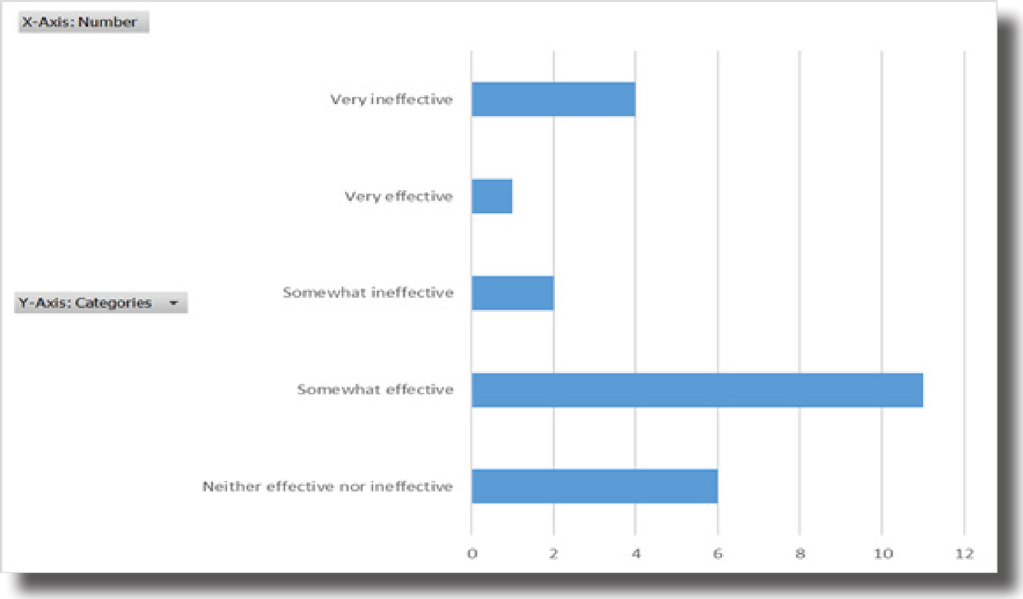
In addition to expert interviews, we also collected information concerning current coordination efforts for and perceived needs regarding critical infrastructure protection in metro Atlanta through an online survey. We used the survey to get an initial sense of where coordination could be improved, to identify additional stakeholders who should be part of our coordination efforts, and to recruit Portal members. (see Appendix D for the survey).

The survey respondents represented a variety of organizations with just under 50% from the private sector, 11% from academia, 11% were individuals, 7% were from non-profits, 4% each from the Georgia state government, the federal government and the military.

Asked about critical infrastructure policies or plans in place at their organizations, one-third (36%) of represented organizations reported having plans, policies and critical infrastructure POC, nearly 29% having policies, 14% having critical infrastructure POC only, 14% plans and policies, and 7% with plans only.

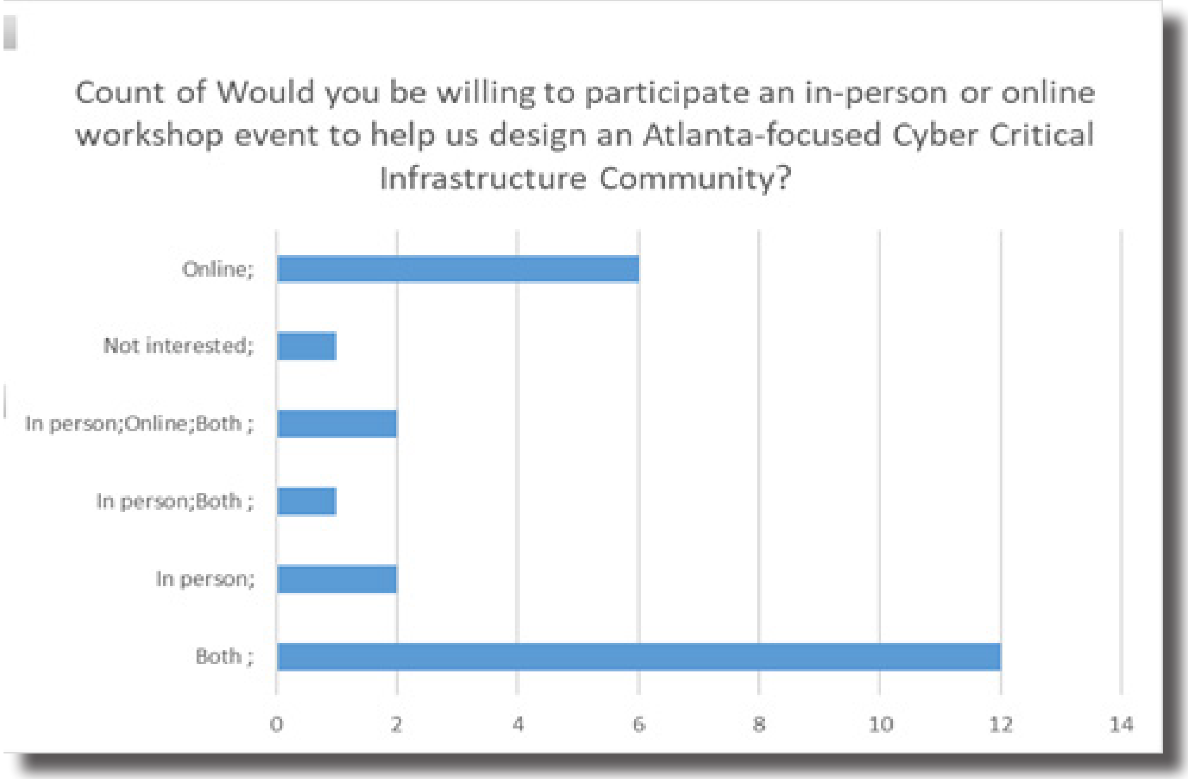
The survey responses regarding the effectiveness of coordination varied, with nearly half (n=12) identifying it as “somewhat effective”, a quarter (n=6) finding it “somewhat or very ineffective”, and another quarter (n=6) as “neither effective nor ineffective”. Only 1 respondent identified coordination efforts as “very effective”.

Survey Participants assessments: Efficacy of current coordination efforts



When asked if they ”would participate in an online or live event to co-design Atlanta C-CIC,” half of the respondents (n=12) stated interest in participating in both online and live events, while one-quarter (n=6) preferred to engage online only.

Survey participants assessments: Willingness to participate - Workshop



Survey respondents represented a range of organizations including military, private and nonprofit sectors, academia, and state government). While we did not detect a pattern in the level of effectiveness of coordination across organization types, we observed similar responses when asked to identify opportunities to improve coordination. The opportunities our respondents identified can be grouped into six categories:

- Community engagement and connections, including improved interaction across agencies (state and federal) and with the broader community and greater connections to resources and in-person events, such as working groups, workshops, and proof of concept implementation.
- Standardized protocols and better monitoring and response to threats to ensure that different organizations use the same guidelines and have a shared understanding of them when coordinating activities.
- Timely and transparent information sharing, such as creating a central cybersecurity information repository containing successes, failures and best practices.
- Improved education on risks for the public and other decision-makers for greater informed awareness and investment in better preventative measures.

Process and Results

In all, we invited a total of 12 agency, organization, academic, and commercial/consulting cybersecurity professionals to test the C-CIC Portal while simultaneously being on a virtual call with TRENDS Global team members in which they shared their initial reactions/feedback while entering the Portal for the first time. We conducted four review sessions with eight veta testers.

The beta testers were generally enthusiastic about the potential application of the Portal. Several observed that the Portal would be a different and new way to share information in Georgia across sectors and agencies. They suggested it could be used in multiple ways such as for meetings, posting jobs, having discussions or distributing products and newsletters. Testers were also interested in the ability to establish private and controlled spaces in the Portal for specific groups with restricted membership, while also being able to engage with the larger community. They also saw potential for the Portal to be expanded to include a broader audience and/or more states.

> *We're trying to get (other state agencies and enterprise agencies) to be really interactive spaces like this, that is kind of a little bit more public. You know, they may be more likely to come here and share and postings, and maybe it could be good.*
> *----State Agency Representative----*

The reviewers also provided helpful feedback. While the specifics of the feedback varied depending on their experience with Portal design, generally their feedback fell into two categories:

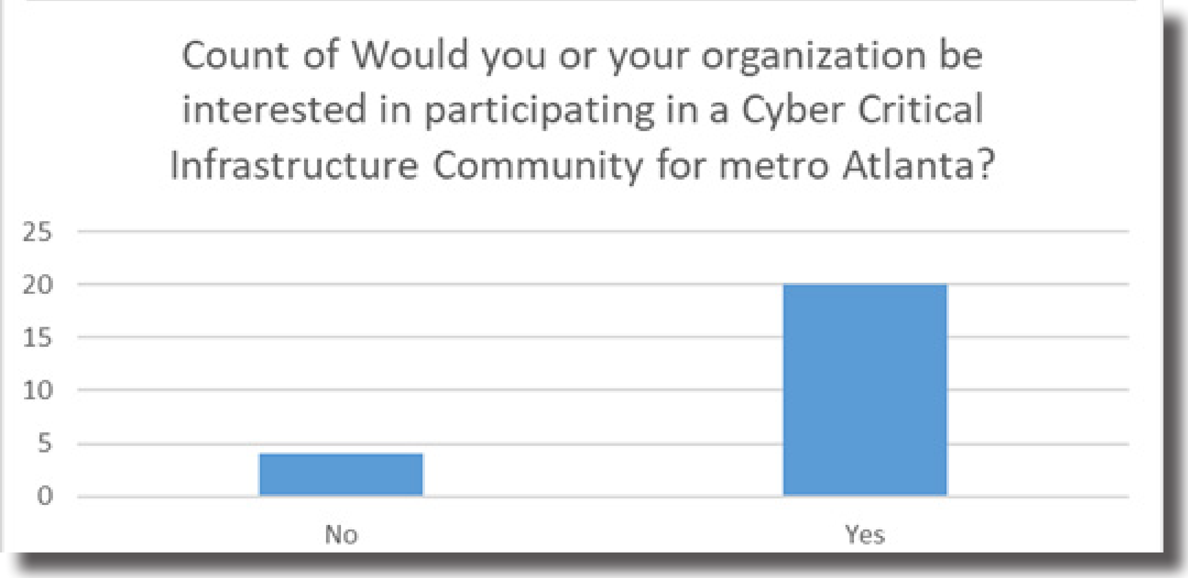
1. Issues that could be resolved with more explanation and guidance in the Portal itself. These issues were not related to the design or functionality but rather to topics such as the kind of information that could/should be shared in the Portal, and to what extent information that is shared is private and inaccessible to nonusers.

2. Suggestions on how the Portal could be improved. The general focus of this feedback was on some design features, navigation, and access. For instance, users have to join each section before they can participate, some sections were set to hidden, which should have been accessible to all users, and some questions about the various features, like what happens when someone follows a member. We shared this feedback with the Portal designer who will make modifications to improve the user experience.

The goal of the Portal is to be functional and useful for a broad range of users and, as such, having the perspective of first-time users exploring the Portal helped us identify key areas of improvement in its functionality so that the Portal can best serve the needs of its users.

When asked if they or their organization would be interested in participating in a cyber critical infrastructure community for metro Atlanta, over three quarters (83%) said yes.

Survey participants assessments: Willing to participate - Community



Stakeholder Feedback

The final step in the Portal development and community engagement process was to invite community members to explore the Portal and share feedback. Once the initial draft of the Portal was operational, we invited cybersecurity community members representing a broad range of institutions/organizations to participate in a live review of the Portal. The reviewers were selected primarily based on their knowledge and involvement in the cyber critical infrastructure industry and interest in the Portal. We sought to invite those who represented a cross-section of the sector/industry. Our one exception was Dr. Amanda Reinke Associate Professor of Conflict Management and an expert in culture, cultural conflict, and community building. Once identified, they were invited to a virtual meeting in which they shared their screen with the project team while interacting with the Portal and sharing their initial reactions. In the test session, participants also had the chance to ask questions and provide real-time feedback on the ease of Portal navigation, structure, and design, and any additional comments and ideas for further improvements (see Appendix E for a list of review sessions and dates).

> *…my unit goes and does physical security assessments and resiliency assessments for critical infrastructure partners. And something we get questioned about a lot is information sharing. And “can I talk to other people who are in the sector and see what they’re going through and what they’ve got going on?” And while sometimes that may not be cybersecurity based, sometimes it is, we arelooking to add a cybersecurity professional to our team shortly, so that could segue nicely into this space. But also if we decided to, you know, host a sub-board for, you know, the energy critical infrastructure, and then they could connect together if they chose to.*
>
> *----State Agency Representative----*

Early Adoption of the C-CIC Portal

Members joined the portal through beta testing, invitations by beta testers to colleagues, and invitations to Atlanta AFCEA. At the time of this writing, the platform, the C-CIC Portal, has the following members:

SECTOR	NUMBER OF PEOPLE
Government	5
Private Sector	12
Academia	3
Team Members (TRENDS/SherpaWerx)	(7)
TOTAL MEMBERS	21
TOTAL INCLUDING HOSTS	28

Ongoing and Continuous Engagement

During the initial research, design and implementation of the C-CIC Portal, SherpaWerx participated in ongoing and continuous engagement with a broader community of cyber-critical infrastructure stakeholders. These engagements have taken place in a variety of ways: through Armed Forces Communications & Electronics Association International (AFCEA) meetings, conferences, and cybersecurity exercises. The goal of these engagements has been to continue building our network of critical infrastructure professionals, learn more about the community and its needs and wants, and find opportunities to talk about the Portal.

For example, we held initial conversations about an online community-based platform that could attract visitors from the private, public, and nonprofit sectors. These were held during the Homeland Security Critical Infrastructure Conference in June 2024, where 30 participants also engaged in a Jack Voltaic exercise. Similar cybersecurity exercises were held at various AFCEA events throughout 2023 and 2024, providing additional opportunities for us to learn more about the cyber critical infrastructure community and gauge interest in developing a platform. These exercises continue to be planned and executed, enabling us to share the C-CIC Portal and discuss its potential role in enabling better critical infrastructure preparedness at the local level.

Deliverables: Cyber Critical Infrastructure Community (C-CIC) Web-based Online Community

This project aimed to develop and deliver a structure and process for a virtual Cyber Critical Infrastructure Community (C-CIC) for the metro Atlanta area. Two elements were developed: the web-based C-CIC Portal and an App. The Portal was developed with community engagement and outreach in mind. As such, the Portal was designed and adapted in response to direct community feedback in an effort to meet the needs of the community as identified in the literature, and in our interviews and the survey.

Summary and Next Steps

The Cyber Critical Infrastructure Community (C-CIC) Portal is a pioneering initiative enhancing the cybersecurity landscape of metro Atlanta by creating a dynamic online community supporting those dedicated to protecting civilian critical infrastructure. It allows key cyber actors to safely share, discuss, and assess security needs, threats, risks, best practices, capacities, emergency protocols and interdependencies. Leveraging cutting-edge technology, the C-CIC Portal enables local governments, academia, the private sector, and nonprofit stakeholders to coordinate and respond to emerging cyber threats more effectively.

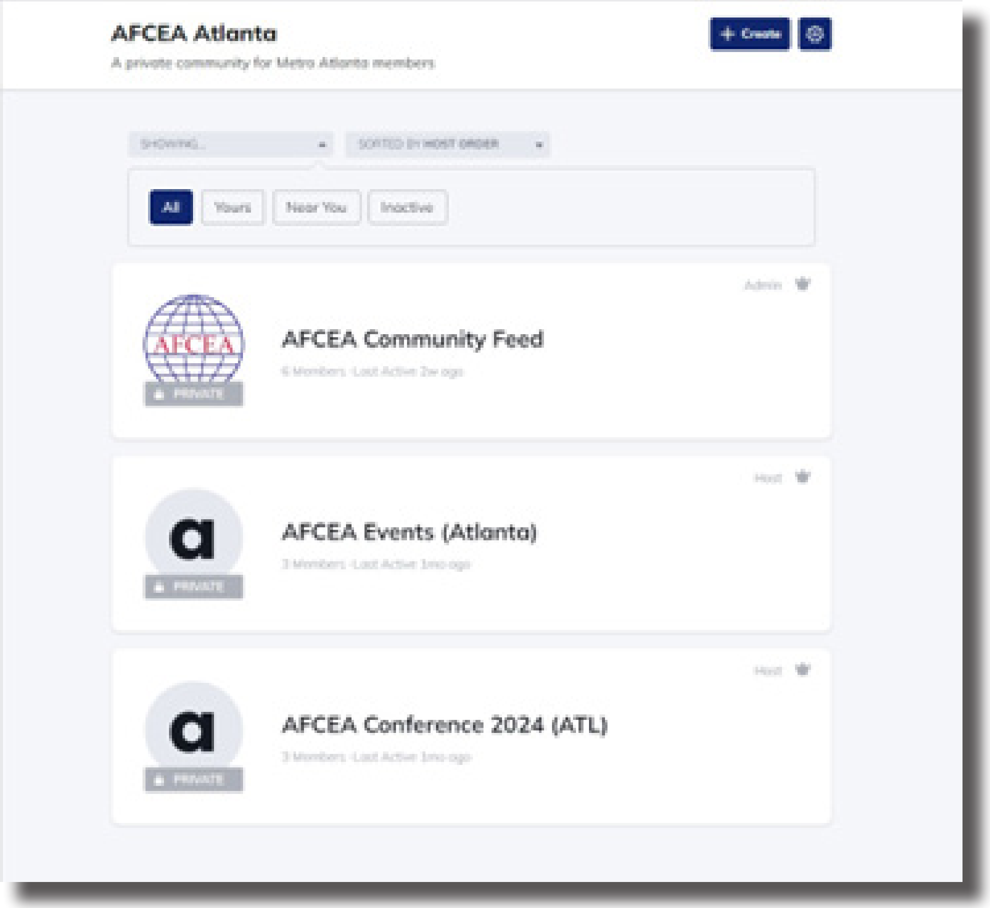
As an inclusive collaboration platform, the C-CIC Portal facilitates knowledge sharing, resource exchange, and best practice dissemination across domains, fostering innovation and alignment in protecting critical infrastructure. The goal of the Portal is to support interest-based groups and private and controlled subgroups, enhancing collective expertise and problem-solving capacity. For local governments, cross-sector collaboration provides diverse insights and solutions, aiding in addressing local cybersecurity challenges more effectively.

We have developed the technological architecture for the Portal and have begun populating it with content based on feedback received from an online survey and a series of interviews with cybersecurity professionals and ACI consortium partners. The community within the Portal has also begun to grow. Overall, reactions have been positive and supportive, acknowledging the need for better and more broad-based information-sharing and coordination of efforts.

Beyond the Pilot: Expanding Cyber Connections

Feedback from cybersecurity professionals and test users indicates interest in and support of our efforts to create an interactive, cyber-focused information and collaboration Portal. Encouraged by the positive responses, extending the C-CIC project to maintain and grow the Portal would be an ideal next step for this project. In a subsequent phase, we would expand the content and reach of the Portal by populating the different Portal hubs (e.g., education, training, skills building, employment, research, events, and policy) and offer additional controlled and private spaces where subgroups can meet and coordinate efforts. We would also develop a fee/membership structure to sustain the Portal through community engagement and funding.

Private AFCEA Subgroup



AFCEA Atlanta

A private community for Metro Atlanta members

AFCEA Community Feed

6 Members · Last Active 2w ago

AFCEA Events (Atlanta)

3 Members · Last Active 1mo ago

AFCEA Conference 2024 (ATL)

3 Members · Last Active 1mo ago

We envision the Portal to be self-sustaining by the end of the next phase described above. The Portal offers an effective and efficient mechanism to integrate schools and universities, rural areas, small businesses, and nonprofits that often lack the necessary cyber resilience into a growing network of actors better prepared to respond to cyber threats. Although small businesses are attractive targets for cyber attacks, they typically lack the security infrastructure of large corporations. Moreover, they typically cannot afford professional IT solutions, have limited time to devote to cybersecurity, or do not even know where to begin. This is where the C-CIC Portal comes in. It equips members, irrespective of organizational size and financial ability, with tools for effective collaboration, including document sharing, learning best practices, conducting risk assessments, and designing response plans. The training hub could be a place to offer Jack Voltaic-inspired exercises.

We also envision expanding the reach of the Portal from the metro-Atlanta area to the state of Georgia and invite state and federal agencies to observe, participate, and help us take the idea of a virtually connected online community to better protect the nation's critical infrastructure to other parts of the country with the intent to eventually build an intentional nationwide network of cyber security professionals and organizations. Key points to support program continuation include:

1. Enhancing Cybersecurity Landscape: The C-CIC Portal was created to engage and support the cybersecurity community in ways not done before. We created a space to share information and collaborate with the goal to better protect the nation's critical infrastructure. We piloted the Portal in Atlanta and received positive feedback and support from cybersecurity professionals and ACI consortium partners who expressed a strong desire for improved information sharing and coordination in cybersecurity efforts.
2. Inclusive Collaboration Platform: The Portal connects diverse actors across sectors, helping with shared resources and information dissemination with the explicit goal of protecting critical infrastructure. The plan is to expand content and reach during Phase 2 and demonstrate a clear path for growth. In Phase 2, we intend to develop various hubs (education, training, research, etc.) and offer private spaces to focus on collaboration, aligning the feedback and needs identified during initial surveys and interviews.
3. Jack Voltaic: Since cybersecurity exercises based on the Jack Voltaic framework have successfully engaged participants across disciplinary, professional and sectoral boundaries, the stage has been set to duplicate efforts using the Jack Voltaic approach across the United States. The data captured by the Portal can create space to enhance the exercise and promote collaboration across participants. For instance, United States Coast Guard Admiral Vann expressed a desire to host these exercises at each of the ports under his authority. An event that would include multiple locations (Atlanta, Savannah, and Augusta) has been requested and is being evaluated. The data from all these events could be stored on the Portal and accessed by anyone who wanted to conduct research. In addition, the Portal will provide a ready-made audience for many of the Army Cyber Consortium projects and research, as well as qualified beta-testers for existing and future projects.
4. Addressing the needs of small businesses and nonprofits which are often vulnerable to cyber threats due to limited resources and expertise. The C-CIC Portal can host tools for collaboration and cybersecurity resilience. Small businesses and nonprofits often lack professional IT solutions and time for cybersecurity. By offering services and resources like document sharing, best practices, and training hubs (potentially including exercises like the Jack Voltaic-inspired scenarios), the Portal fills critical gaps in cyber resilience for these groups and may offer additional revenue streams.
5. Sustainability and Community Engagement: The Portal has the potential to provide a long-term approach for strengthening cyber resilience. The Portal is positioned to become self-sustaining with the development of a fee/membership structure and ongoing community engagement. This approach aligns with similar successful models in other community-driven cybersecurity initiatives, like All Partners Access Network.

Summary and Next Steps

6. Expansion Beyond Atlanta: With continued funding, we plan to expand our community-building efforts by extending access to the Portal beyond metro Atlanta. The successful pilot in Atlanta serves as a proof of concept, suggesting that communities elsewhere, especially those with limited resources, could benefit from adopting the Portal. State agencies, like the Georgia Emergency Management Agency, could include more rural areas that do not have the funding to engage full-time cybersecurity teams. During our interview, GEMA representatives posed the idea of transmitting information, best practices, guidelines, etc. via a subgroup in the Portal. We have tested and confirmed that this is achievable.

The C-CIC Portal not only addresses current cybersecurity challenges in metro Atlanta but also has a well-defined strategy for growth and sustainability. Positive feedback from Beta testers and stakeholders and the identified needs of underserved stakeholders like local governments, military bases, small businesses, and nonprofits underscore the importance of continuing and expanding this initiative beyond the current performance period.

Project Maturation

This project is part of TRENDS Global's ongoing efforts to bring research rigor to the design and implementation of community programs. The TRENDS approach focuses on identifying and engaging key stakeholders from the community early in the process and, with their input, creating multiple mechanisms for community input and feedback at all stages, from design to implementation, and evaluation.

In addition to the additional steps outlined above, the Portal has the potential to have a broader application. The model that was used to develop the current Portal could be replicated for other critical infrastructure communities and even other types of issue-focused communities, with members identifying the needs of their community and the TRENDS Global team creating a dedicated virtual community space. Additionally, the benefits of each C-CIC community could be expanded further by creating private and controlled spaces for interactions of specific groups within the broader community.

Convinced of the utility of the C-CIC Portal after the successful pilot, we are developing a proposal to disseminate to likely Portal users and potential funders, including state organizations like the Georgia Emergency Management Agency (GEMA) and AFCEA International.

The C-CIC Portal has not only generated interest among Atlanta-based cyber professionals but also from ACI consortium partners. The TRENDS Global team has begun conversations with Dr. David Schwartz from the Rochester Institute of Technology to develop a research proposal for submission to the National Science Foundation. In the proposal, we intend to combine behavioral research and gaming to study the nature and impact of decision-making in simulated crisis scenarios deployed on a gaming platform hosted by the Portal to develop community resilience.

Building an online community of cybersecurity professionals presents challenges, particularly in fostering trust, engagement, and effective collaboration. Trust and a sense of belonging can, however, arise through interactions over time, especially when this is combined with common experiences, successes, and failures. The C-CIC Portal is aimed at cultivating a vibrant, cohesive community of cybersecurity professionals, with the goal of encouraging timely and authentic communication, collaboration, and a sense of belonging among members. All our efforts to build effective online communities are rooted in the in-person community-building practices described above.

Integrating coordinated in-person workshops within this virtual C-CIC framework can significantly enhance the community's overall efficacy and cohesion. Research has demonstrated that trust is a fundamental component of effective virtual teams, and it can be significantly bolstered through in-person interactions, which are vital for deepening trust and resolving miscommunications, misunderstandings and complex, interpersonal issues. In-person interactions can bridge gaps in trust and make virtual collaborations more robust.   By leveraging the strengths of both virtual and physical interactions, a hybrid approach ensures that the community can effectively tackle complex challenges while fostering a supportive and cohesive professional network.

The existing Jack Voltaic exercise framework can be adapted both as a virtual game on the Portal as well as at in-person gatherings. A sense of locality can be created by focusing on local issues in the exercises themselves and also by encouraging members to organize and participate in local meetups, networking events, or casual get-togethers by providing a dedicated space for members to announce, plan and discover events in their area.

The insights gained from implementing a hybrid model in the next C-CIC phase can inform scalable frameworks for other domains and provide valuable data for future online community building. For instance, insights from this project and its hybrid implementation can be strategically integrated into virtual communities in academia, finance, manufacturing, and logistics.

Based on the lessons learned from the C-CIC pilot, we believe building a virtual or hybrid community of cyber professionals and their organizations can be an effective way to strengthen the resilience of America's critical infrastructure to prevent, reduce and respond to domestic and foreign threats. We also believe there is great need and potential for C-CIC-building in other parts of the country and propose to formalize a structure that allows the Jack Voltaic concept to be repeated in a systematic way that produces consistent benefits (through experiences and data points). An ideal outcome would be the development of a self-sustaining and scalable ecosystem to help keep our critical infrastructure safe and secure for generations to come. The current project has developed a solid framework for strengthening America's cyber resilience. TRENDS Global and SherpaWerx stand ready to utilize the C-CIC Portal to grow the list of resilient cyber critical infrastructure communities.

ENDNOTES

1. The Atlanta metro area was defined in line with how the Atlanta Regional Commission describes it here: https://atlantaregional.org/about-arc/about-the-atlanta-region/

2. See Franke and Guidero (2012) for a conceptual model for stakeholder engagement that has informed the TRENDS approach: https://www.semanticscholar.org/paper/Engaging-Local-Stakeholders%3A-A-Conceptual-Model-for-Franke-Guidero/86a219014f3db3d074510366ca02a009f37f7290

3. See Franke and Guidero (2012) for a conceptual model for stakeholder engagement that has informed the TRENDS approach: https://www.semanticscholar.org/paper/Engaging-Local-Stakeholders%3A-A-Conceptual-Model-for-Franke-Guidero/86a219014f3db3d074510366ca02a009f37f7290

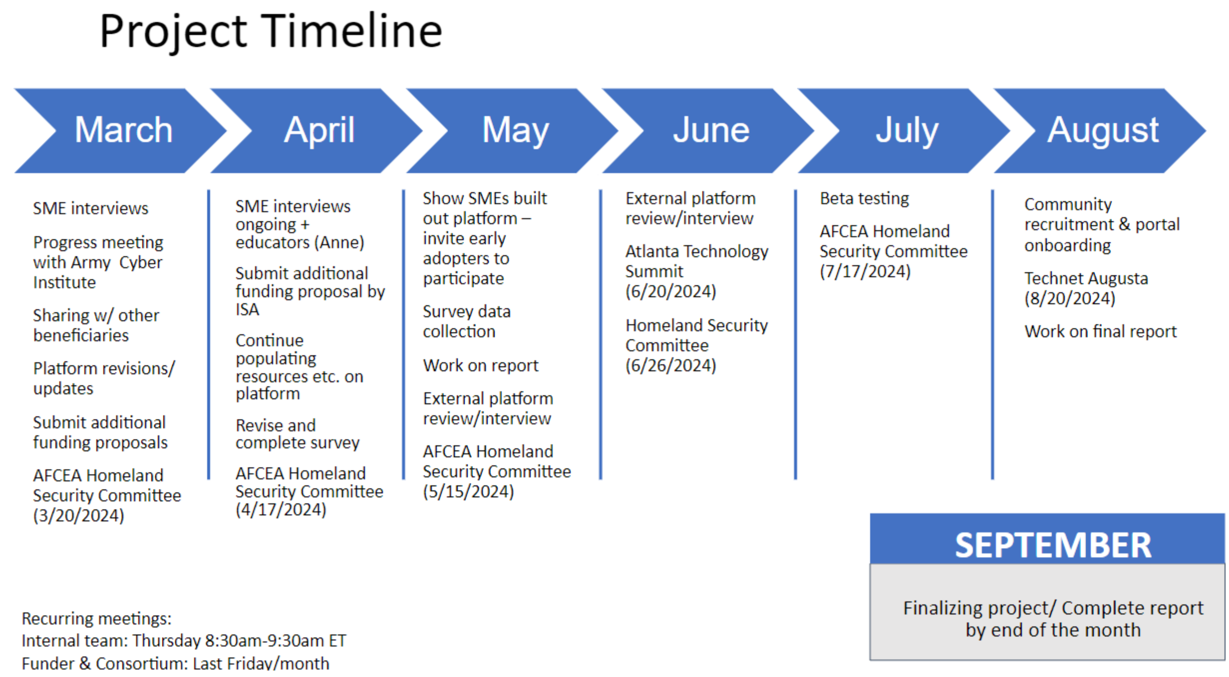
4. M. Alves et al., “Can Virtuality Be Protective of Team Trust? Conflict and Effectiveness in Hybrid Teams,” Behaviour & Information Technology 42 (2022): 851–68.

5. Katharina Gläsener, Thomas Afflerbach, and Antoinette Weibel, “Trust and Distrust in Hybrid Virtual Teams - Perceptions of Trustworthiness across Subgroup Boundaries,” 2014

APPENDICES

APPENDICES

APPENDIX A: PROJECT TIMELINE



Project Timeline

March

SME interviews

Progress meeting with Army Cyber Institute

Sharing w/ other beneficiaries

Platform revisions/ updates

Submit additional funding proposals

AFCEA Homeland Security Committee (3/20/2024)

April

SME interviews ongoing + educators (Anne)

Submit additional funding proposal by ISA

Continue populating resources etc. on platform

Revise and complete survey

AFCEA Homeland Security Committee (4/17/2024)

May

Show SMEs built out platform – invite early adopters to participate

Survey data collection

Work on report

External platform review/interview

AFCEA Homeland Security Committee (5/15/2024)

June

External platform review/interview

Atlanta Technology Summit (6/20/2024)

Homeland Security Committee (6/26/2024)

July

Beta testing

AFCEA Homeland Security Committee (7/17/2024)

August

Community recruitment & portal onboarding

Technet Augusta (8/20/2024)

Work on final report

SEPTEMBER

Finalizing project/ Complete report by end of the month

Recurring meetings:
Internal team: Thursday 8:30am-9:30am ET
Funder & Consortium: Last Friday/month

APPENDIX B: LITERATURE REVIEW

By Lina Tuschling and Timo Zwarg

Community building has evolved significantly with the advent of digital platforms, leading to the formation of robust online communities that complement or even substitute traditional in-person communities. Early online communities of the 1990s, for example, were often characterized by a comparatively high level of emotional investment and commitment compared to larger social network environments like Instagram or Twitter/X. However, tight-knit groups, "positive, democratic, communal 'places'" in the online sphere continue to exist. In general; however, use of networks is moving from close-knit, tight relationships to "more far-flung, expedient, and diverse personal networks" (Kozinets 2019).

The concept of "community" varies across cultures. For many Americans, the prototypical communities are small towns and religious congregations—groups where people interact regularly and share common interests. However, other cultures may have different ideal models of community (Bruckman 2022).

Kraut et al. (2012) define online communities as any virtual space where individuals come together to converse, exchange information or resources, learn, or simply connect with one another. These communities can take many forms, ranging from small, close-knit groups to large platforms with millions of participants. The defining characteristic of an online community is the presence of ongoing interactions among members, some of which are mediated by technology. The technologies supporting these communities are diverse, including email lists, forums, blogs, wikis, and social networking sites. Despite these differences in platform and scale, the central focus of online communities remains sustained interaction over time, which is essential for their longevity and success.

An effective online community requires several key elements to foster meaningful engagement and sustained participation: A sense of belonging is essential, as successful communities help members feel connected through multi-faceted networks and authentic interactions, distinguishing them from social media platforms that often emphasize consumption. These communities are typically built around a shared niche or purpose, providing members with a clear reason to engage. At the heart of any thriving online community are organic, user-driven conversations, which contrast with host-generated content that may dominate other platforms. For the community to function smoothly, the platform must be well-organized, making it easy for members to find relevant content and providing tools for hosts to manage the space effectively. Community leadership is also crucial, with active hosts or leaders guiding members toward common goals and shaping their experiences. Additionally, online communities offer unique content that stands apart from what can be found on traditional social media platforms, further encouraging participation. Finally, real engagement is marked not by superficial interactions, such as likes or brief comments, but by conversations that evolve and move forward through active member involvement. (Mighty Networks, "Online Community")

Managing Online vs. In-Person Communities

Online communities offer opportunities for support and engagement, particularly in situations where physical presence is impractical. Russell et al. (2022) examined the role of online communities in providing support to individuals with long COVID and highlighted the role of virtual spaces in offering emotional and informational support.

The comparative analysis of online and in-person communities reveals distinct advantages and challenges associated with each. Online communities offer accessibility and convenience, enabling participation independent of physical location, and favoring continuous engagement. However, they may face issues related to user retention and the depth of engagement compared to in-person interactions, which often benefit from stronger emotional connections and immediate feedback.

When considering how communities manifest online, key considerations include what aspects of face-to-face communities offer meaningful support, how online platforms can be designed to provide similar value to their members and what new forms of support online interactions can offer that are not possible in face-to-face settings (Bruckman 2022).

A key distinction for online communities is the transient nature of their membership. Many members of online communities remain active only until they reach specific goals or lose interest, which presents a challenge for sustaining engagement over time. Without a regular influx of new members, online communities are at risk of stagnating and eventually dying out (Ng, 2011).

The organizational structure of online communities must reflect both key aspects of what defines an online community: the social dimension of a group of people and the technological dimension of interacting online. Achieving a careful balance between these two is essential in designing an online space that encourages community members to organically create and sustain their community from the ground up. It should incorporate essential features that help "weave" a community together with each user shaping their own experience within the online community, without being constrained by externally imposed rules, while at the same time, the space must establish boundaries for social interaction to prevent chaos (Glezakos and Lazakidou 2012).

Thematic categorization of the literature indicates that successful online communities often leverage:

- **Inclusivity and Cultural Sensitivity**: Ensuring that community engagement strategies are tailored to the cultural and social contexts of the members (Oliveira et al., 2022).
- **Motivation and Support Systems**: Facilitating peer support and providing motivational resources to sustain engagement (Santo et al., 2021).
- **Strategic Partnerships**: Collaborating with academic, governmental, and community organizations to enhance the credibility and reach of the online community (Cantwell, 2021).

By focusing on inclusivity, motivation, and strategic partnerships, online communities can effectively complement traditional in-person interactions, providing robust platforms for support, engagement, and collective action.

Charles Vogl, in his book *The Art of Community* (2016), discusses advanced ideas for managing both face-to-face and online communities. Vogl emphasizes that community leaders should understand the types of success people seek: relative success, personal maximization, and community maximization. Leaders aiming for community maximization prioritize the success of the group over individual gains, fostering a more cooperative and resilient community environment. On the subject of leadership, Ng (2011) argues that a well-managed community, guided by an effective community manager and supported by clear guidelines, is better equipped to sustain member engagement and grow over time, mitigate the transient nature of online communities and proactively address challenges such as member attrition and competition from other platforms.

Engaging directly with members is also key to building a sense of community. Millington (2021) recommends that community managers interact with members personally, responding to their posts, facilitating discussions, and showing genuine interest in their contributions.

Vogl (2016) also applies seven principles to online communities to enrich them, highlighting the importance of clear group identity, proportional benefits, and costs, collective decision-making, effective monitoring, graduated sanctions, accessible conflict-resolution mechanisms, and the right to organize.

Kwak (2016) highlights the importance of centrality, reciprocity, and core-periphery structures in fostering user engagement and sustaining community growth. By understanding these four factors, Kwak argues, community managers can develop strategies to enhance user interactions and create a thriving online community:

1. **Centrality**: Users with higher centrality values play a crucial role in the community's growth. These users, often referred to as "hubs," facilitate information flow and engagement by attracting more interactions. The centrality of users positively correlates

with the duration and number of comments, indicating that central users contribute to sustained community activity.

2. **Reciprocity**: High levels of reciprocity, or mutual exchange of comments, enhance the community's cohesiveness and user engagement. Reciprocal interactions foster a sense of belonging and trust among users, which is essential for community retention and growth. Reciprocity has a significant impact on the duration of user participation, suggesting that mutual interactions encourage users to remain active in the community for longer periods.
3. **Core-Periphery Structure**: The presence of a well-defined core-periphery structure is indicative of a healthy online community. Core users are densely connected and actively participate, while peripheral users contribute less frequently. The growth of the community is heavily influenced by the activities of core users. As core users increase their interactions, they attract more peripheral users, thereby expanding the community.
4. **Duration and Frequency of Interactions**: The duration and frequency of user interactions are critical indicators of community growth. Longer interaction durations and higher frequencies suggest a more vibrant and engaged community. Communities with frequent and sustained interactions are more likely to experience continuous growth, as users remain engaged and contribute regularly.

Factors Contributing to the Success and Failure of Online Communities

Online communities are increasingly essential for fostering collaboration, social interaction, and information sharing. However, the success of such communities is not guaranteed, with many failing to sustain engagement and participation over time. According to Kraut et al. (2012) in *Building Successful Online Communities: Evidence-Based Social Design*, several critical factors contribute to the failure or success of these communities, emphasizing the importance of clear objectives, differentiation from competitors, and achieving critical mass.

Millington (2021) underscores that there is a short window of opportunity after a community's launch to gain traction. Successful communities, he notes, typically reach three key data points within the first three months: 100 contributing members per month, 300 monthly posts, and 10 new registrations per day. Without reaching these early milestones, a community may struggle to generate the activity needed to sustain engagement.

The failure of many communities can be attributed to unclear objectives, insufficient membership, and competition from larger platforms. However, by focusing on carving out a niche, effectively competing within that niche, and reaching critical mass, communities can foster the engagement and sustained participation necessary for long-term success. (Kraut et al., 2012).

Rewarding members for their contributions is a central theme in Millington’s (2021) strategy for community building. He identifies four primary types of rewards that can help motivate members and keep them engaged:

1. **Reputation**: Offering members recognition in the form of badges or featuring them in community content builds their status within the community.
2. **Access**: Providing members with exclusive access to private groups or internal contacts can foster a sense of privilege and inclusion.
3. **Influence**: Empowering members by offering moderator roles or soliciting their feedback on community design and content helps strengthen their commitment.
4. **Tangible rewards**: Offering physical rewards such as branded swag, discounts, or training opportunities can provide additional motivation for members to stay engaged (Millington, 2021).

Taking a Hybrid Approach

Alves et al. (2022) explore the protective role of virtuality in team trust, noting that cognitive trust is a critical antecedent of team effectiveness in hybrid teams. Their study suggests that while virtual environments can shield teams from some conflicts, in-person interactions remain vital for building deeper trust and resolving complex interpersonal issues. Integrating coordinated in-person workshops within a virtual framework can significantly enhance a community's overall efficacy and cohesion. Research has demonstrated that trust is a fundamental component of effective virtual teams, and it can be significantly bolstered through in-person interactions, which are vital for building deeper trust and resolving complex, interpersonal issues.

This finding aligns with Gläsener et al. (2014), who highlight the importance of trustworthiness across subgroup boundaries in hybrid virtual teams. They argue that in-person interactions can bridge gaps in trust and make virtual collaborations more robust.

Research into blended learning environments, as explored by Namyssova et al. (2019) indicates that combining digital and in-person educational strategies enhances engagement and learning outcomes. This blended approach ensures that members of the community not only acquire technical knowledge but also develop strong interpersonal relationships and trust, which are critical for effective collaboration in high-stakes environments.

Social capital (Putnam 2000) is fostered through both strong ties (close relationships) and weak ties (Granovetter 1973), with weak ties being particularly valuable for providing broader access to information and opportunities Online platforms, through social media and other computer-mediated communication, are especially suited to maintaining and expanding weak ties, and thus enhance bridging social capital. Moreover, online interactions not only build social networks but also often lead to increased face-to-face interactions, making online and offline community engagement mutually reinforcing (Bruckman 2022).

Millington (2021) emphasizes the importance of keeping conversations active and creating ongoing content to sustain member interest. Hosting and facilitating both online and offline events is a powerful way to keep the community vibrant.

Integrating in-person workshops within an online community of cybersecurity professionals can significantly enhance trust, engagement, and collaborative efficacy. By leveraging the strengths of both virtual and physical interactions, a hybrid approach ensures that the community can effectively tackle complex cybersecurity challenges while fostering a supportive and cohesive professional network.

As we have seen, online communities have evolved significantly, transitioning from the close-knit groups of the early Internet era to more expansive, diverse networks today. While these communities differ from traditional face-to-face gatherings, they retain essential features like *ongoing interactions*, *shared purpose*, and a *sense of belonging*. Effective online communities achieve meaningful engagement through user-driven conversations, strategic leadership, and clear organizational structure. However, they face challenges such as user retention, cultural differences, and competition from larger platforms Leaders play a crucial role in shaping community success by encouraging engagement through rewards, recognition, and facilitation of both online and offline events. Theories on social capital, particularly the strength of weak ties, highlight the power of online networks in expanding bridging capital, which helps members access broader resources and opportunities. *Integrating online and in-person interactions* can enhance community engagement by reinforcing trust and collaboration, a strategy supported by research on hybrid approaches.

References:

Alves, M., I. Dimas, P. Lourenço, T. Rebelo, V. Peñarroja, and N. Gamero. 2022. “Can Virtuality Be Protective of Team Trust? Conflict and Effectiveness in Hybrid Teams.” *Behaviour & Information Technology* 42:851–68.

Borowiec, Katrina, Deoksoon Kim, Lizhou Wang, Juli Kim, and S. Wortham. 2021. "Supporting Holistic Student Development Through Online Community Building." *Online Learning*.

Bruckman, Amy S. 2022. *Should You Believe Wikipedia?: Online Communities and the Construction of Knowledge*. 1st ed. Cambridge University Press. https://doi.org/10.1017/9781108780704.

Ghamrawi, Norma. 2022. "Teachers' Virtual Communities of Practice: A Strong Response in Times of Crisis or Just Another Fad?" *Education and Information Technologies* 27:5889–5915.

Gläsener, Katharina, Thomas Afflerbach, and Antoinette Weibel. 2014. "Trust and Distrust in Hybrid Virtual Teams - Perceptions of Trustworthiness across Subgroup Boundaries." In . https://www.semanticscholar.org/paper/bb6ab38ede73bd6edc6f00ef1929f0d7b90f5e78.

Granovetter, Mark S. 1973. "The Strength of Weak Ties." *American Journal of Sociology* 78 (6): 1360–80. https://doi.org/10.1086/225469.

Kozinets, Robert. 2019. *Netnography: The Essential Guide to Qualitative Social Media Research*. 3rd edition. Thousand Oaks, CA: SAGE Publications.

Kraut, Robert E., Paul Resnick, Sara Kiesler, Moira Burke, and Yan Chen. 2012. *Building Successful Online Communities: Evidence-Based Social Design*. Cambridge, MA: MIT Press.

Kwak, Nayeon. 2016. "An Study on Determinants Affecting a Growth of Online Community." In *International Journal of Computer Applications*, 12:163–69.

Lazakidou, Athina A., ed. 2012. *Virtual Communities, Social Networks and Collaboration*. Annals of Information Systems, v. 15. New York: Springer.

Lazakidou, Athina A., and Nick Glezakos. 2012. "Organizational Design of Online Communities." In *Virtual Communities, Social Networks and Collaboration*, edited by Athina A. Lazakidou, 61–74. Annals of Information Systems, v. 15. New York: Springer.

Matsumoto, Yuichi, Hiroki Kasamatsu, and M. Sakakibara. 2022. "Challenges in Forming Transdisciplinary Communities of Practice for Solving Environmental Problems in Developing Countries." *World Futures* 78:546–65.

Mighty Networks. n.d. "Online Community." https://www.mightynetworks.com/encyclopedia/online-community.

Millington, Richard. 2021. *Build Your Community: Turn Your Connections into a Powerful Online Community*. First edition. Harlow, United Kingdom: Pearson Education Limited.

Namyssova, Gulnara, G. Tussupbekova, Janet Helmer, K. Malone, Mir Afzal, and D. Jonbekova. 2019. “Challenges and Benefits of Blended Learning in Higher Education.” In , 2:22–31. https://www.semanticscholar.org/paper/3177063809e0e50b4618f135ca51d798cb63c4c6.

Ng, Deborah. 2011. *Online Community Management For Dummies*. Hoboken, NJ: For Dummies.

Nicolini, Davide, Igor Pyrko, O. Omidvar, and Agnessa Spanellis. 2022. “Understanding Communities of Practice: Taking Stock and Moving Forward.” *The Academy of Management Annals*.

Putnam, Robert D. 2000. *Bowling Alone: The Collapse and Revival of American Community*. Simon and Schuster.

Russell, D., N. J. Spence, J. Chase, T. Schwartz, C. M. Tumminello, and E. Bouldin. 2022. “Support amid Uncertainty: Long COVID Illness Experiences and the Role of Online Communities.” *SSM - Qualitative Research in Health*. https://www.semanticscholar.org/paper/bad4beb4401b00a5632f4257cbad880d2c71f574.

Shaw, L., Dana Jazayeri, D. Kiegaldie, and M. Morris. 2022. “Implementation of Virtual Communities of Practice in Healthcare to Improve Capability and Capacity: A 10-Year Scoping Review.” *International Journal of Environmental Research and Public Health* 19.

Smith, Karen. 2021. “Contact, Connection, and Communication: Online Community Building on a Professional Doctorate.” *Journal of Learning Development in Higher Education*.

Vogl, Charles. 2016. *The Art of Community: Seven Principles for Belonging*. Oakland, CA: Berrett-Koehler Publishers.

APPENDIX C: INTERVIEW SCHEDULE

Date	Subject	Context
Mar 1, 2024	Klint W.	Local Cyber Actor
Mar 11, 2024	Joye P.	Local Cyber Actor
Mar 14, 2024	Kristen Pedersen	Consortium
Mar 15, 2024	Jim Dempsey	Consortium
Apr 3, 2024	Scott Schackelford	Consortium
Apr 4, 2024	Carter S.	Local Cyber Actor
Apr 12, 2024	Dave Schwartz	Consortium
Apr 22, 2024	Nate L.*	Local Cyber Actor
Apr 23, 2024	Kathy S.	Local Cyber Actor
Apr 26, 2024	Ed P.*	Local Cyber Actor

*Interview not be completed

APPENDIX D: SURVEY

Metro Atlanta Cyber Critical Infrastructure Community Survey

With funding from the Army Cyber Institute, SherpaWerx and TRENDS Global research how to develop and grow communities to support those involved with the protection and security of civilian critical infrastructure. The research assesses critical security needs, existing capacities, interdependencies, resilience, impact of disruptions, and overall protection of these critical resources.

We are interested in assisting the development of a Cyber Critical Infrastructure Community for metro Atlanta by strengthening existing relationships, networks, and processes. As a starting point, we would like to learn more about what you perceive to be the most critical security needs and what you would be looking for in a Critical Infrastructure Community.

Please take a few minutes to answer the following questions as honestly as you can. There are no right or wrong answers. Please take as much time as you need to answer each question.

Please note, for research purposes, we will keep your answers strictly confidential unless expressly agreed otherwise. For data analysis purposes, we will assign numbers to participants that will be used on all research notes and official documents. You can skip questions you do not want to answer and stop the survey at any point.

For questions and suggestions regarding this project or the instrument, please contact our

Research Team:

- Dr. Volker Franke, Executive Director, TRENDS Global, Email: volker@trendsglobal.org
- Paul Wertz, Chief Executive Officer, SherpaWerx, Email: paul@sherpawerx.com

- Dr. Anne Chance, Research Associate, TRENDS Global, Email: anne@trendsglobal.org
- Dr. Amanda Guidero, Research Associate, TRENDS Global, Email: amanda@trendsglobal.org

Informed Consent

Research at Trends Global that involves human participants is carried out under the oversight of an Institutional Review Board. Questions can be directed to info@trendsglobal.org.

Please answer the following questions (* indicates response is required)

1. Are you 18 years or older? *

- Yes
- No

2. Please indicate the following consent to participate. *

- I agree and give my consent to participate in this research project. I understand that participation is voluntary and that I may withdraw my consent at any time without penalty.
- I do not agree to participate and will be excluded from the remainder of the questions.

Survey

3. What are the biggest threats to/needs for critical infrastructure protection in metro Atlanta? Please list up to 3 threats and/or needs and explain why you think they are important. *

4. How would you assess the effectiveness of current practices to coordinate efforts among individuals and organizations involved with the protection and security of civilian critical infrastructure in metro Atlanta? *

- Very effective
- Somewhat effective
- Neither effective nor ineffective
- Somewhat ineffective
- Very ineffective

5. How could coordination be improved (what works well and what doesn't) *

6. Please list organizations, agencies, businesses, or individuals you think should be part of a Cyber Critical Infrastructure Community for metro Atlanta and how committed you think they are to coordinating efforts with other critical infrastructure actors.

To assess their commitment, please write in the letter you think best describes the organization or individual’s commitment to actively participate in a metro Atlanta Intentional Critical Infrastructure Community:

1. Their purpose/mission is to protect the critical infrastructure of the community as a whole.

2. Their purpose/mission is to solve a particular critical infrastructure problem or protect only a particular critical infrastructure area.

3. Their purpose is to serve themselves by generating benefits for the community. They are willing to take risks to do so.

4. Their purpose is to serve themselves and their benefits weaken the community.

Please list all actors you think are important to include in a metro Atlanta Intentional Critical Infrastructure Community, not just those you think are most excited to participate, and assess their level of commitment to participate in such a community.

7. Would you be willing to participate in an in-person or online workshop event to help us design an Atlanta-focused Cyber Critical Infrastructure Community?   *

- In person
- Online
- Both
- Not interested

8. Would you or your organization be interested in participating in a Cyber Critical Infrastructure Community for metro Atlanta? *

- Yes
- No

9. If yes, please provide your name or the name and email address of the person or persons to invite: *

Demographics

Please fill out the following demographic information.

10. What agency/organization do you represent? (enter N/A if you do not wish to answer)

11. What category best describes your organization?

- Federal Government
- State Government
- County Government
- Municipal Government
- Military
- Private Sector
- Health Care Facility
- Academic Institution
- Non-Profit/Civil Society Organization/NGO
- Media
- Individual
- Other

12. What, if any, critical infrastructure policies or plans does your organization have in effect? Check all that apply:

- Plans
- Policies
- Critical infrastructure security POC

APPENDIX E: REVIEW/BETA TESTING SCHEDULE

Session date	Number of reviewers	Number of TRENDS Global representations
May 31, 2024	1	2
June 6, 2024	3	2
Aug 13, 2024	1	2
Aug 16, 2024	1	2