Fragile Foundations Sprint

Thursday September 3rd, 2026

AGENDA

1. Welcome and Introductions
2. Why We Are Here
3. Fragile Foundations Sprint
4. The Broader Context
5. Get involved!

Whoarewe?

Josh Corman
Executive-in-Residence
Public Safety & Resilience, IST
Founder, I Am The Cavalry

Jen Ellis
Adjunct Policy Advisory, IST
Founder, NextJenSecurty

David Batz
Critical Infrastructure
Protection Advisor

Daniel G. Alvarez
Program Coordinator, IST

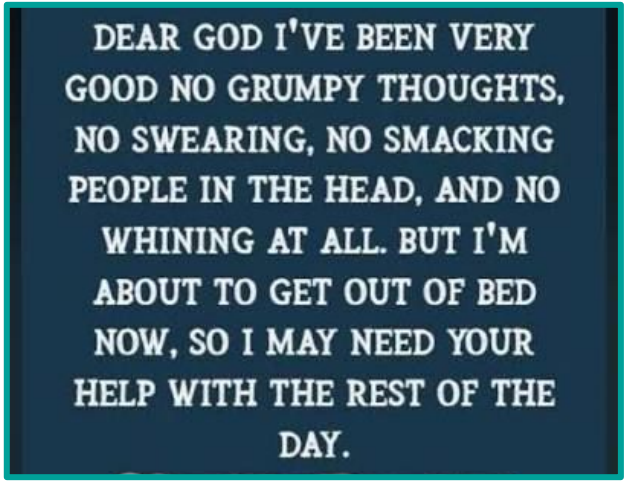
Introducing the Fragile Foundations Sprint

Confronting AI cyber disruption to life-safety critical functions.

- Focused specifically on cyber-poor operators in life-safety critical functions
- 5 work streams focused on pragmatic outcomes
- 100 days (Sept 3 - Dec 10)
- Collaboration of OT/ICS, cybersecurity, AI, engineers, operators, policymakers
- Practical guidance now; groundwork for additional future engagement

Principles for Engagement

- Participate in an authentic and active way.
- Be considerate and respectful, even when challenging information or points of view.
- Avoid demeaning, discriminatory, or harassing behavior and speech.
- Refrain from pitching your products/services, no matter how awesome they are!
- Treat information shared with appropriate sensitivity and confidentiality.




CHAMPIONS
USA 250
SUPER BOWL LX
CHAMPIONS
SEAHAWKS


SHORT & MASON LTD.
LONDON
NW
NE
W
E
SW
SE
S

5 CHICAGO LOCAL WEATHER VIDEO INVESTIGATIONS ENTERTAINMENT SPORTS NBC 5 RESPON... 80° Watch 24/7

TRENDING 24/7 Streaming News Chicago Sports Must-See Videos Chicago Today Matt in the Morning Open House Chicago Roeper's R...

INFRASTRUCTURE

Government admits water system cyberattacks were worse than first reported

The Iran war is bringing cyberwarfare into critical infrastructure

Recent attacks in the UK and the US demonstrate critical vulnerabilities that governments need to urgently address.

CISA confirms hackers targeted over 100 US water systems during July

CYBERSECURITY DIVE Deep Dive Library Events Press Releases

Newly identified hacking groups provide access to OT environments

DEFENSESCOOP Topics Events Podcasts Vide

Air Force cyber leader warns threats like Volt Typhoon could enable China to wage 'total war' against US

Cyber threats against operational technology networks are growing, Lt. Gen. Thomas Hensley said.

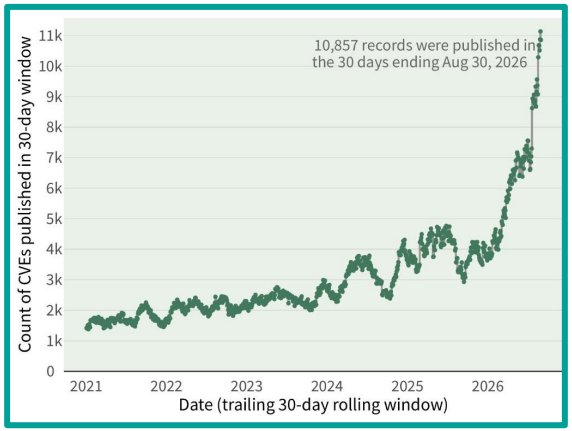
China's 'Typhoon' cyber operations target US critical infrastructure sectors in move toward large-scale disruption

AI is supercharging hacks of everyday utilities

Evolving Threats to Our Life-Safety Critical Functions

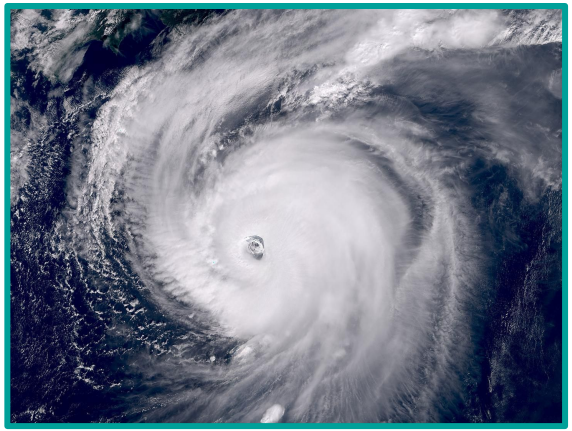
Iran Conflict
Current

AI-Discovery & Exploitation
Current-ish



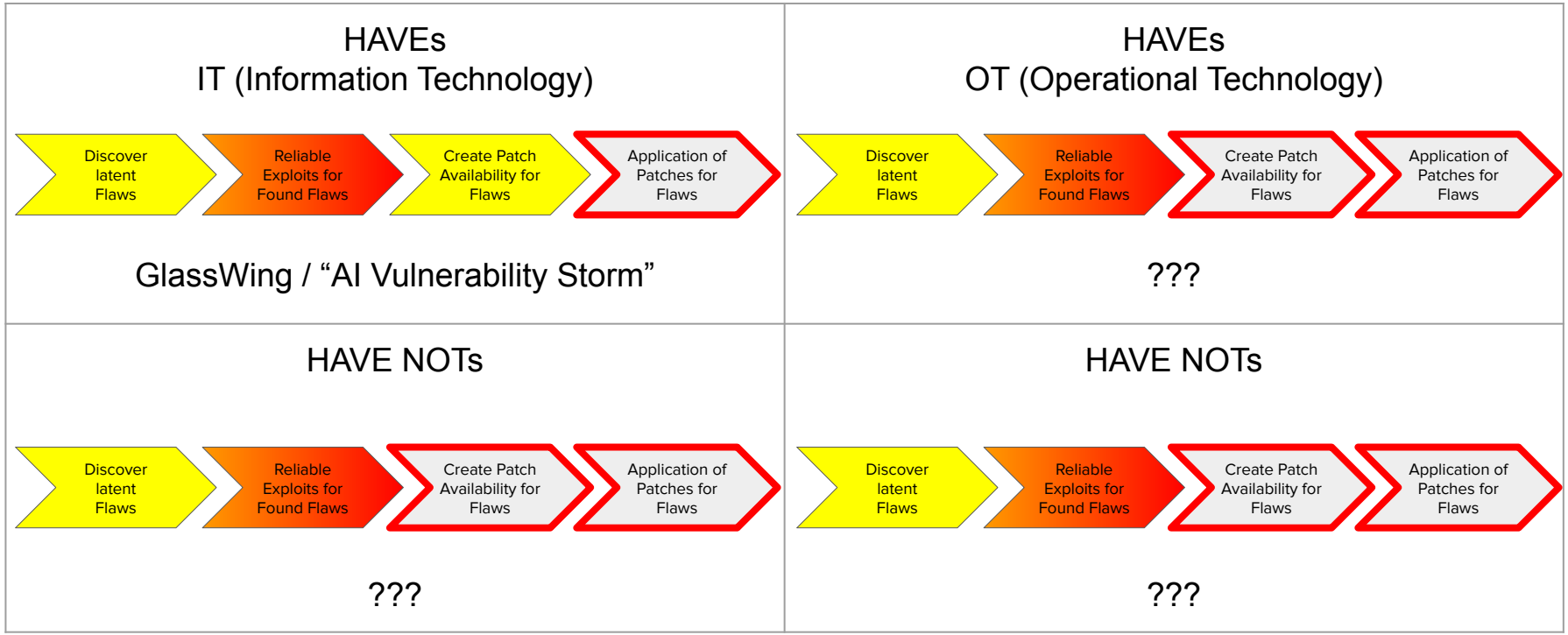
Source: Jay Jacobs, Empirical Security

Taiwan Conflict
2027-2030




CORPORATE
IT
PROJECT
GLASSWING
MUNICIPAL
WATER SYSTEM

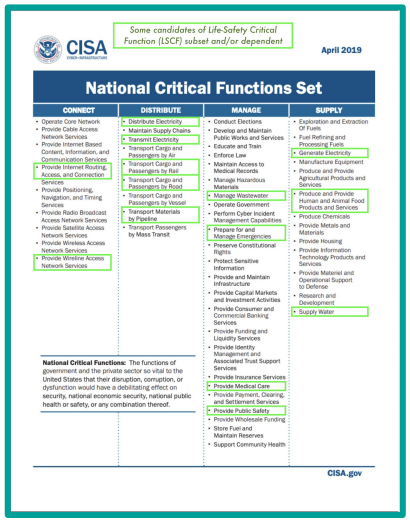
A Concerning Bias in AI Focus




NO WATER
NO HOSPITALS
NO KIDDING
UNDISRUPTABLE27.ORG

What do we mean by “Life-Safety Critical Functions?”

“The fundamental services and infrastructure required to maintain human health, safety, and the economy during a disaster.”



- Generate, distribute, and transmit electricity
- Supply water and manage wastewater
- Provide medical care and maintain access to medical records
- Provide public safety
- Prepare for and manage emergencies
- Produce and provide human and animal food products and services
- Transport Cargo and Passengers by Rail
- Transport Materials by Pipeline
- Provide Wireline Access Network Services; provide Internet Routing, Access, and Connection Services

Source: https://www.cisa.gov/national-critical-functions-set

LSCF operators are “**cyber-poor**” if they lack either:

- **Incentives** (market forces, regulation, grants, etc)
- **Information** (education, engagement, etc)
- **Resources** (personnel, financial, materials, etc)

In some cases, they may be lacking all three.

Realities of OT/ICS environments

- **Availability is king, followed by integrity, then confidentiality.**
- **The importance of a critical function includes the sum of its downstream impacts to other critical functions.**
- **Threats may come from cyber, but solutions often come from engineering.**
- **Best practices for IT should not be assumed relevant to OT environments.**
  - ➢ The fragility of OT/ICS systems mean many cybersecurity best practices won't work and may cause harm.
- **Legacy tech and tech debt are common. Lifecycles for OT can span decades. Costs are considerably higher than enterprise tech.**
- **There has been a push towards connectivity, often without consideration to exposure and risk.**
- **Patching is notoriously difficult, in part due to the fragility of systems and intolerance towards disruption.**
  - ➢ Patching a system may violate the terms and conditions of the system integrator
  - ➢ In this era, where it is important to patch faster, unpatchable equipment is unsafe

Challenges and constraints for Cyber-Poor Operators

- **Many have almost no money or availability of cyber talent. They may have engineering capability.**
  - ➢ Free cybersecurity is “free as in puppies” so can still be challenging.
- **Many utilities are price-fixed locally or at the state level, and even a federal push may not survive contact with existing regulatory price constraints.**
- **Systems integrators can be resistant to change or outside interference. Contracts may prohibit pro-security activity such as patching.**

Goals for the Fragile Foundations Sprint

- Engage and educate cyber-poor operators on pragmatic measures for confronting AI cyber disruption in the near term.
- Develop and document understanding of challenges and opportunities for building resilience against AI cyber disruption in cyber-poor LSCF operators.
- Equip policymakers and leaders to confront AI cyber disruption to cyber-poor LSCF operators.
- Establish solid foundations for others to build on to create greater resilience for cyber-poor LSCF operators.

Working Groups and Co-Chairs

Consequences analysis		Mark Montgomery		Éireann Leverett
OT/ICS sector engagement		Alison King		Mike Holcomb
Pragmatic guidance for cyber-poor operators		Whitney Bowman-Zatzkin		Samara Moore
Novel mitigations analysis		Michael Daniel		Art Manion
Policy and incentives design		Matt Hayden		Megan Samford

Consequences Analysis

Description

When everything is critical, nothing is critical. This group will examine which US National Critical Functions are most consequential when disrupted (esp life-safety), how the disruption of these critical functions affects other dependent critical functions (2nd & 3rd order effects), which are most vulnerable, and which are typically least resourced. Once identified, it should assess/ characterize the relative preparedness of each responsible sector's public-private partnership - as well as headwinds and tailwinds to improving resilience. Lastly, it will make recommendations for preventing and/or responding to the domino effects of disruption and restoring service as quickly, efficiently, and effectively as possible.

Tasks

1. Explore consequences of disruption across life-safety critical functions. Include analysis of interdependencies and cascading effects of disruption.
2. Highlight risk profile of cyber-poor entities in LSCF - where are the targets and why? Develop a risk map to document this.
3. Examine current sector preparedness/resilience, including identifying and documenting the relevant factors of evaluation.
4. Document resourcing realities covering spectrum of factors (awareness/ engagement; financial; people; etc).
5. Develop recommended response path in the event of various crisis scenarios.
6. Collaborate with OT/ICS Sector Engagement, Policy and Incentives WGs.

Deliverables

1. Detailed write up of the WG process and findings, including focus areas, decision-making factors, and response recommendations.
2. A list of the most consequential NCF disruptions on their own.
3. Mappings of which NCFs depend upon each other, revealing/suggesting
4. Prioritised risk map for our highest priority NCFs for resilience/recovery efforts

OT/ICS Sector Engagement

Description

Identify and engage major OT/ICS suppliers, smaller-but-vital sector-specific systemically-important entities (SIE), system integrators and key service providers. Expose gaps in engagement or support for LSCF cyber poor operators. Evaluate preparedness for assessing and responding to the needs of the cyber-poor (rather than better-funded orgs). Drill into specific aspects of support/engagement that add extra friction or offer resilience benefits, e.g., legacy and entrenched tech debt, exploring whether AI will only worsen gaps or could also offer potential solutions, and examining whether SBOMs can be meaningfully adopted for impact analysis from a larger volume of CVE and exploits. Aimed at the highest consequence communities, the group will also propose options for better supporting the most at-risk customers (e.g. Cash for Clunkers to replace/update unsupported tech with patchable tech… e.g. prioritizing assistance/response/simulations).

Tasks

1. Map vendor ecosystem roles and document engagement models, barriers-to-adoption or engagement, and incentives (good and bad) shaping the way these entities support cyber-poor LSCF operators.
2. Document evaluation of industry willingness/suitability to support cyber-poor operators. Develop recommendations for boosting engagement and support.
3. Build additional deep analysis on key issues, for example tech debt, SBOM.
4. Explore opportunities to engage with AI frontier model producers to evaluate/strengthen the technologies used most amid high consequence LSCF operators.
5. Collaborate with/suggest inputs for Consequence Analysis, Pragmatic Guidance, and Policy and Incentives WGs

Deliverables

1. Initial inventory & ecosystem map of important cross-sector AND sector-specific suppliers smaller-but-vital suppliers, systems integrators & service providers most depended upon across LSCFs..
2. Detailed summary of analysis including discussion of incentives, challenges, and current status. Include a wish-lists for how frontier models can help the suppliers.

Pragmatic Guidance for Cyber-Poor Operators

Description

This group will explore the realities of cyber-poor LSCF environments and develop realistic, pragmatic, actionable, jargon-free guidance for operators that lack access or suitability for standard cybersecurity recommendations. These organizations are unlikely to deploy AI-powered defenses. They may be unable to adopt any standard security practices. The group will need to assess which guidance is broadly applicable cross-sector, and which is specific to the LSCFs. There may be multiple sets of guidance developed, depending on timing and focus of the group. Some of the help can be "top 3 questions for your: Equipment vendors, System Integrators, Insurers, etc." Model Contract addendums might be a useful input to Policy and Incentives Design.

Tasks

1. Explore limitations of conventional cybersecurity 'best practices' or frameworks for cyber-poor OT/ICS environments.
2. Identify alternative, more realistic approaches to leverage engineering.
3. Determine structure/strategy for guidance and identify pragmatic recommendations, documented in a manner that is easy-to-use and appropriate to the target audience. Test guidance for suitability with cyber-poor operators and adjust as needed.
4. Ensure terminology alignment and if necessary, provide lexicon/glossary of terms. (e.g. hazard analysis, not threat model).
5. Coordinate with the Sector Engagement and Novel Mitigations Working Groups to ensure alignment and intel sharing.

Deliverables

1. Segmented or cross-sector guidance(s) - leaning towards talent pools and resources (e.g. engineering). Suggest top-line strategies about unsound dependence. Produce "N Critical Questions for your (Suppliers, Integrators, Insurers, etc)." Glossary / mapping of terms.
2. Craft prioritized resources lists.
3. Documentation of analysis and decision-making processes.

Novel Mitigations Analysis

Description

This group will surface and evaluate novel mitigation strategies proposed for the growing volume, variety, and velocity of AI-era disruptions. The group must embrace unconventional thinking for problem solving in unresourced and mission-critical environments. The group will develop a framework for evaluating the practicality and viability of novel mitigations, which may vary by sector or other organizational factors. This will help prioritize recommendations. Considerations should include: legal, ethical, effectiveness, scalability, speed, proven track record, and where authority sits. Are there pre-conditions or the potential for collateral damage? Exploring and assessing existing proposals may help catalyze better ideas.

Tasks

1. Capture new and existing - possibly controversial - unconventional ideas for dealing with increasingly dangerous connectivity and exposure.
2. Develop and apply an analysis framework to determine viability of proposals. Explore the fragilities of OT/ICS operators to understand less obvious consequences of each idea.
3. Prioritize mitigations based on practicality and suitability.
4. Coordinate with the Pragmatic Guidance and Policy and Incentives Working Groups to ensure alignment.

Deliverables

1. Document analysis and decision-making process. Cite third party proposals for unconventional mitigations as well as the group's own suggestions.
2. Create an initial list of novel mitigations - scored against your analytical/viability framework.
3. Include recommendations to Policy and Incentives WG to support the adoption of the most pragmatic and suitable mitigations.

Policy and Incentives Design

Description

This group will explore the realities and incentives across LSCF ecosystem stakeholders and document the factors driving barriers to adoption of resilience. The group will examine how different constraints (pricing, staffing, resources, supply chain, awareness, incentives) drive exposure, vulnerability and fragility across cyber-poor operators. The group will brainstorm public policy approaches to identify, realign or replace perverse incentives. They will consider the viability of approaches to restore resources or circumvent their lack. They will consider how best to equip policymakers and other leaders to take action on these issues. This group will collaborate with the other working groups to align recommendations that will accelerate adoption of mitigations and remove structural barriers.

Tasks

1. Explore realities of cyber-poor operators to understand limitations of conventional mitigations for these environments.
2. Brainstorm policy and other interventions to realign incentives, remove barriers-to-adoption of pragmatic mitigations to increase LSCF resilience. Audiences can include local, state, federal legislators and regulators.
3. Collaborate with Consequence Analysis, Sector Engagement, Pragmatic Guidance, and Novel Mitigations Working Groups to reflect and align with their recommendations. Identify gaps in their approach and work on solutions/recommendations to address them.
4. This group could directly engage with policymakers to carry the mission forward.

Deliverables

1. Document the priority outcomes/equities needed by cyber-poor LSCFs.
2. Analysis of misaligned and/or perverse incentives and barriers-to-adoption of resilience, with corresponding recommendations for policy or other remediations.
3. Legislative cheat-sheets and briefings; public and private evangelism of recommendations (in collaboration with IST).

WG Kick-off calls

Consequences analysis	Mark Montgomery Éireann Leverett	Friday, September 4th 09:00 ET/ 06:00 PT (sorry!)
OT/ICS sector engagement	Alison King Mike Holcomb	Friday, September 4th 11:00 ET/ 08:00 PT
Pragmatic guidance for cyber-poor operators	Whitney Bowman-Zatzkin Samara Moore	Friday, September 4th 12:00 ET/ 09:00 PT
Novel mitigations analysis	Michael Daniel Art Manion	Friday, September 4th 13:00 ET/ 10:00 PT
Policy and incentives design	Matt Hayden Megan Samford	Thursday, September 3rd 15:00 ET/ 12:00 PT

Considerations for WGs

- Disruption may be due to second order impact of an attack (i.e. your organization was not the direct target of the attack)
- It's not about the size of the entity. It’s the size of the harm that matters. (e.g. not population of water plant’s town; supports only hospital w/in 150 miles)
- When it comes to life-safety, an unmitigated pathway to harm is sufficient to trigger a corrective action
- Lack of historical attacks should not be comforting; we have predators who want to disrupt even if not for financial interests

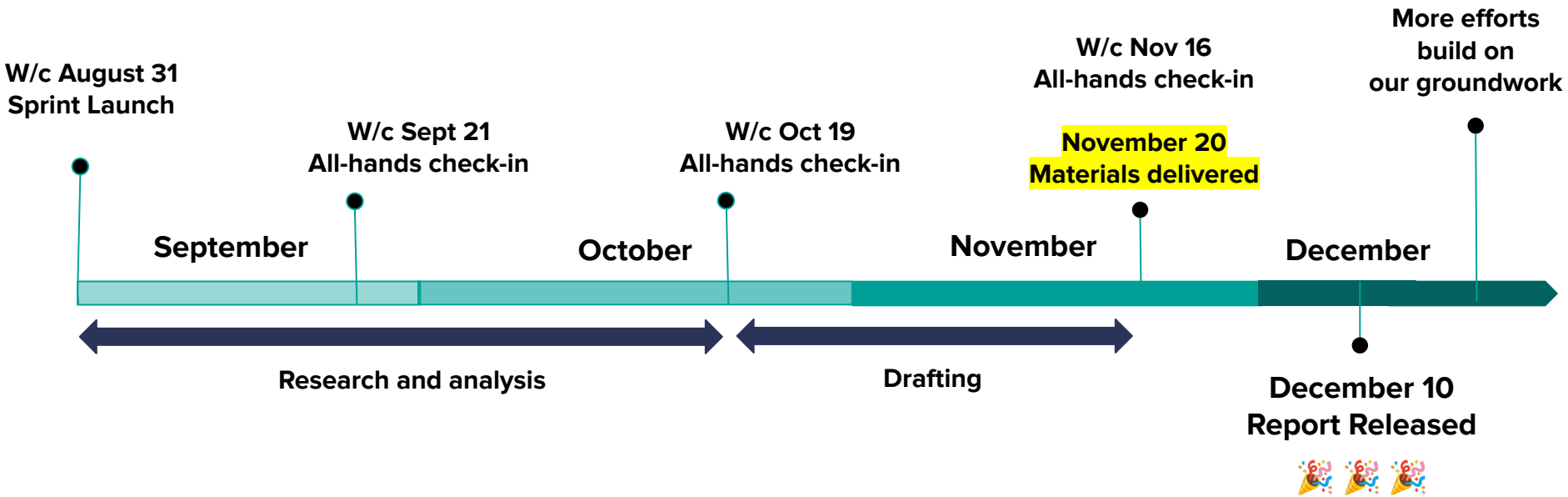
Commitments, Coordination and Information Sharing

- Participate in weekly WG calls (choose your group) and other WG commitments
- Co-chairs alignment call every 2 weeks
- All-hands alignment and milestone check-in every 3-4 weeks
- Interview opportunities with cyber-poor operators
- WG, co-chairs, and general channels in UnDisruptable27 Slack workspace

Sprint Deliverables

- **Report detailing each Working Group's efforts, including:**
  - Summary of process
  - Explanation of decision-making, including influencing factors, assumptions, and evidence
  - Description of outcomes
  - Recommendations for future progress
- **Accompanying assets from specific Working Group processes (Risk Map, Ecosystem Map, Mitigations Framework)**
- **Pragmatic guidance documents for cyber-poor operators**

Timeline and Milestones



The Broader Context

Related-but-separate distinct projects, funders etc.

- UnDisruptable27.org (Craig Newmark Philanthropies)

Related AI work across IST

- AI Risk Barometer
  - https://securityandtechnology.org/ai-risk-barometer/
- AI Risk Reduction Initiative
  - https://securityandtechnology.org/ai-risk-reduction-initiative/
- AI Recursive Self-Improvement
  - https://securityandtechnology.org/blog/ist-launches-rsi-initative/
- AI Agents and Agency
  - https://securityandtechnology.org/virtual-library/white-paper/ai-agents-agency-in-the-internet-ecosystem/

Next Steps

Interested in participating?

- Review the WGs and choose which to join: FragileFoundations.org
- Register your interest at: https://form.jotform.com/262367406420049
- Check out/share the video of the FF100 Kick-Off Webinar: https://www.youtube.com/watch?v=oNbamKoa_JU
- Encourage others to join in too!

THANK YOU for giving your time and expertise to this important effort.

Together we can create change.