Summarized notes (Thank you to (b)(6))

Overview: CISA has limited capabilities to identify, track disinfo narratives + attempts to undermine confidence in elections

- SIO does = good partnership
- Major goal: prevent a crisis of confidence in 2020 elections
    - E.g., where Russia doesn't change any votes (or changes just a few), but claims they changed many more and hysteria is blown out of proportion

Scope: Keep scope narrow: focus on election-related disinfo that has the potential to impact the public's voting patterns

Partnerships and Relationships: SIO would be the coordinators, working w/ Graphika, DFRLab, and (b)(6) (b)(6)s team at UW

- Mutual trust is key: don't want to need NDAs, legal red tape
- Need to build out workflow management system: JIRA/Slack/other communications channels, shared processes and definitions, etc.
    - (b)(6) envisions Tier 1 and Tier 2 partners
    - Tier 1 is intake (of tips, disinfo reports, etc.): consisting of people either digging for narratives, or processing info received from other partners
        - Think students, election officials, etc. who are looking for disinfo
        - Workflow: check that info against protocols, do some initial data aggregation, triage it into the workflow management system
    - Tier 2 is the 4 orgs: (b)(6) team at Stanford, Graphika, etc.
        - Workflow: take stuff off the workflow management queue, process it
        - Need to sketch that out
        - SLA for different times of the calendar based on the level of severity obtained by triage
            - E.g., a report from the general public will have less priority than a report from an on-the-ground election official; a report for disinfo that is not popular will have less priority than disinfo that is going viral
            - General public = more turnaround time, but election officials = less turnaround time: need to get back to them fast
- SIO has good relationship w/ platforms who already care
    - See the Secondary Infektion (Russian disinfo op) report
        - Think through all the platforms that might have been useful there (e.g., communicating with Twitter at stage *x* would have stopped the spread)
- Meanwhile, CISA has strong relationships w/ election officials
    - CISA is happy to introduce SIO to them, do outreach
    - Just keep CISA in the info-sharing pipeline
- SIO normally won't share with intelligence community (IC) or law enforcement
    - No gov't agencies other than CISA
    - CISA is free to converse, triage with IC

  - SIO won't publish or share private info: goal is to find disinfo, not expose suspects behind it
- Regarding the general public: create a workflow to 1) understand, 2) mitigate, 3) communicate
  - Understand a narrative and its theme; ensure it's relevant; identify accounts behind it
  - Then, mitigate it: send details to the platforms and CISA
  - Finally, hopefully it's mitigated by the time we communicate the details to public
  - Need a trustworthy place for general public to go
    - Could be social media, a live blog, or something more complex
    - It'll probably be a live blog with social media: ~2 paragraph statements of what we've found, the accounts affected, note we've forwarded it to gov't + platforms
    - Goal: all organizations involved approve a central statement saying *x* narrative/piece of disinfo is not true and why

Timeline from here: SIO publicly announces the partnership in 2-3 weeks

- Public post about the partnership
- Hold a webinar to talk through everything with election officials + stakeholders
  - Tell them how they can submit tips, give feedback, stay in sync

CISA's concern starts 45 days out operationally, when military/overseas voters start mailing

- Start hunting, messaging at beginning of September
  - Lower SLA (higher turnaround time/less priority), but start looking for search terms and taking tips
- The days leading up to/right after Election Day will be much more intense
- It'll be an effective SOC, maybe a physical one, but in a much larger space

Example scenarios

What if we find a disinfo op in a state SIO hasn't yet built a relationship with?

- CISA can make the introduction, preferably through the ISAC
  - ISAC has a reporting structure where election officials can report tips to platforms
  - CISA can provide SIO those channels
- SIO will publicly disclose the op: it serves as counterspeech, and it reaches relevant officials outside the info-sharing pipeline
  - CISA can decide if it looks foreign, whether to forward it on to IC/other parties

What if official sources post disinfo (e.g. candidate's Twitter)?

- That scenario is out of scope, and even if it's misinfo, it'll still be widely received
- SIO *could* add value if a candidate tweets misinfo about the electoral process
  - Need to discuss: how much do we want to unanimously say this is untrue? Emphasize respected election lawyers' voices? This could get political fast

How would we notify political parties (along with their own stakeholder/notification groups)?

- We'd do it in a completely fair manner and offer services to both of them