Chapter 6 The Disinformation Response Network

A Thousand-Point Solution **1**

Responders **1**

Elves 2

Information Sharing Networks 2

Reaching the networks **3**

ISACs / ISAOs 3

MISP Networks 3

Broadcast from your own network 3

A Thousand-Point Solution

"Disinformation isn't a silver bullet problem, it's a thousand-bullet problem" - Pablo Breuer.

Disinformation is a distributed, heterogeneous problem: there are many incident, narrative and artifact creators, across many different channels and communities. The response to this isn't going to be just from a few large organisations: it will need to come from all of society, and be collaborative, heterogeneous, and connected.

Lots of different groups at lots of different scales will need to work together, and we need to connect them, in a way that respects the groups, the subjects of disinformation, and the accounts and groups being investigated. Practically, that means both finding and connecting those groups, and carefully designing around privacy, sharing, and standards.

Responders

Mostly, when people think about cognitive security, they look at platforms, public, and government as responders. But as we catalogued counters, we found many types of people, resources, and groups who could help. A few of these actors include:

- Other infosec people
- Platforms
- Law enforcement
- Governments and government departments
- Communities and Elves

- Influencers
- Media
- Nonprofits
- Academia and Educators
- Industry / corporations
- General public and individuals

Potential responders include the whole of society, including the infosec bodies already linked by the ISAOs and cyber Interpols. You may find yourself sending reports to, or working alongside, many of these people.

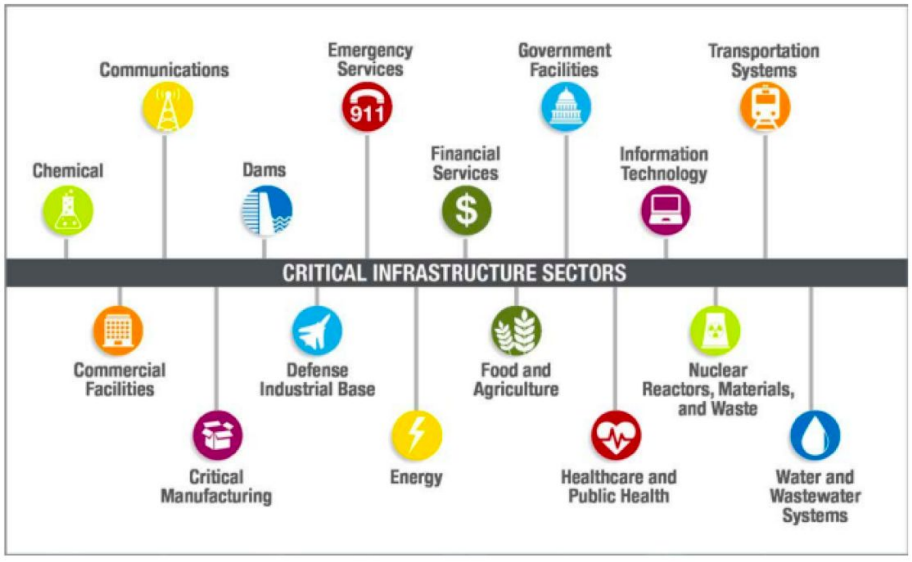
Elves

One group we're focusing on are the Elves. In Eastern Europe, these are volunteer groups who go online to counter Russian troll activities - mostly with tracking, truth and humor. We've been wondering if that could work elsewhere and set out to support it.

References:

Elves vs Trolls: fighting disinformation in Lithuania

Information Sharing Networks



ISACs (USA)

A group that we support is the information sharing and analysis organizations: the ISAOs, ISACs and cyber Interpols. These organizations already share infosec information for critical sectors in the USA, and we now have one that shares cognitive security information to all the

other ISAOs and ISACs: the CS-ISAO (Cognitive Security ISAO), run by IACI-CERT at the Center for Space Education, NASA/Kennedy Space Center, Florida.

References

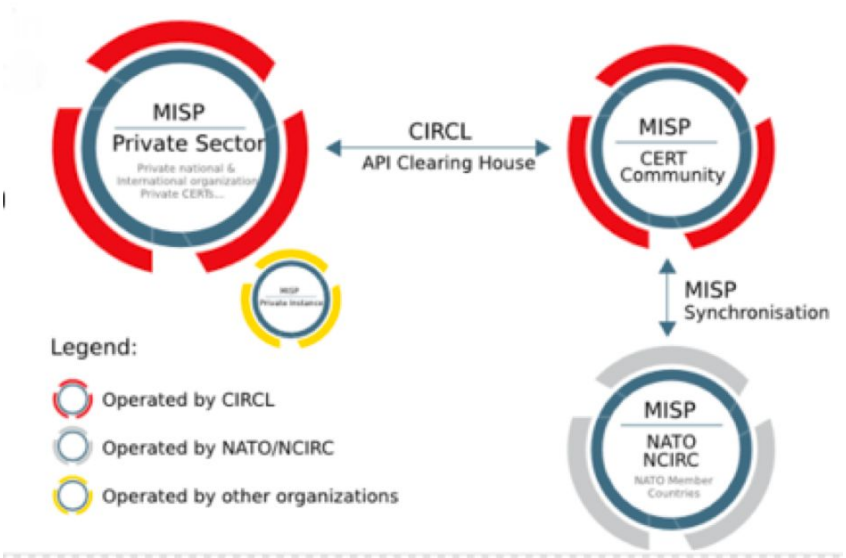
- https://www.isao.org/information-sharing-groups/enrollment/
- https://www.dhs.gov/cisa/information-sharing-and-analysis-organizations-isaos
- https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf

Reaching the networks

ISACs / ISAOs

Although your community or organisation can join an ISAO, the easiest way to these quickly is to find someone who's already part of them. Most of them share information using the STIX data standard (see the disinformation models section), many of them use the MISP platform (see the tools section).

MISP Networks



MISP communities

MISP communities of users and organizations run MISP instances that share information about threats and cyber security indicators worldwide. Many are easy to join; it's also possible to stand up your own MISP instance and add it to the network (see Tools chapter). MISP communities include: EU, ISAC, ISAO, CERTs, CSIRTs, NATO, Military, Intelligence, Fortune

500s. Misp connections include API push/pull, email out, and connections to other tools (e.g. Anomali ThreatStream, ThreatConnect, OSQuery).

CogSecCollab runs the MISP disinformation community.
https://www.misp-project.org/communities/

Broadcast from your own network

If your community is creating and outputting data, research and other outputs, you could push those out yourself, taking care to respect privacy, not start panic etc etc. In practice, that means sending things like flash alerts through a system that's either part of a larger network (e.g. the MISP networks), or broadcast to subscribers (e.g. email).