1. Cognitive Security

TL;DR: Cognitive Security

- Cognitive security is a holistic view of responses to digital harms from a security practitioners' point of view.
- Cognitive security is one of 3 interacting layers of information security: physical, cyber, and cognitive

Cognitive Security

Cognitive Security, CogSec, uses information security practices to manage digital harms.

Information security, InfoSec, is the protection of information and information systems from unauthorized access, modification or use. InfoSec has three layers:

- **Cybersecurity**: machines and the networks between them
- **Physical security**: breaking into the building, because it's easier to steal from the computer than break in electronically
- **Cognitive security**: human beliefs, human emotions, and the networks between them

A hybrid incident includes two or more of these layers, and may also include components from other security domains, e.g. military actions. The same security principles can be used in each of these layers, customised to fit each layer but retaining enough commonality to monitor and defend against hybrid incidents.

What CogSec Covers

CogSec includes components of infosec like social engineering - manipulating people into taking actions or sharing information, often as part of breaking into a secure system, where classic social engineering techniques include phishing - using emails, phone calls or SMS to obtain private information, and impersonation. One view of CogSec is that it’s “social engineering at scale”.

More recently, CogSec has included responses to information operations, disinformation and other digital harms where information is transmitted between humans, usually via computer networks.

What InfoSec Does and Doesn't Give Us

InfoSec is now more than three decades old. It has a large community and industry around it, that has built tools, techniques and resources for infosec threat sharing and response.

CogSec uses InfoSec practices, processes, frameworks, and tools, adapted for the cognitive domain. These are useful for joining together existing disinformation responses, and for planning and carrying out cognitive security mitigations, responses and remediation:

- **Mitigations** - making successful incidents less likely to happen,
- **Responses** - tracking and reducing the effectiveness of cognitive security incidents,
- **Remediation** - repairing the damage from successful incidents. Using knowledge from them to help make related incidents less likely.

InfoSec includes frameworks - models for thinking about the security of information systems. The "CIA triad" of *Confidentiality, Integrity, Availability* gives:

- **Confidentiality**, not making information available to people who aren't authorized to access it.
- **Integrity**: ensuring that information isn't modified or deleted by unauthorized people.
- **Availability**: ensuring that information is available to authorized people when they need it.

This is a useful frame for thinking about digital harms, for example: Disinformation is an integrity problem[1], and responses to it need to be tempered by the need for information availability. InfoSec also has frameworks, e.g. STIX, for modelling information ecosystems,

[1]Danny Rogers, Fake news as an information security problem, Forbes 2018

and for modelling threat behaviours, mitigations and counters, e.g. ATT&CK and the SANS scale, that we've adapted for disinformation use.

Adapting existing InfoSec frameworks means we can use the same tools as the rest of InfoSec, including open source tools like MISP, to analyse and share information about CogSec incidents and threats.

InfoSec includes processes for defining threats, threat sources, indicators, effects, and potential counters. It also includes ways to organise and run long-term threat monitoring teams.

InfoSec is one of many views of digital harms. Building successful responses to digital harms requires inputs from many disciplines including data science, cognitive psychology, sociology, history, military theory, and marketing. What infosec - via CogSec - provides, is existing frameworks, processes and toolsets that we can use to build defence ecosystems from each of these views.

CogSec Threat Response

Keeping a CogSec response running requires work from three main areas of infosec:

- **Operations**: monitoring, investigating and responding to security threats. Includes Threat Intelligence. Usually near-real-time.
- **Test & Validation**: making a system more resilient to threats. Includes simulations, red teaming, penetration testing, compliance analysis, and exercises. Can be done slowly or periodically.
- **Enablement**: work that prepares for and underpins Operations and Test & Validation. Includes data engineering, data standards, security architectures, and

training. Usually done at the start of a deployment - setting up the teams and systems for response.

Risk management is part of each of these. Finding disinformation online isn't difficult. The art is in placing detection, response, and mitigation resources, to minimise the attack surfaces, vulnerabilities, and potential loss from disinformation.

CogSec Services

The CTI League handbook stresses "Our members prioritize efforts on helping hospitals and healthcare facilities protect their infrastructures during the pandemic and creating an efficient channel to supply these services". The disinformation team should do this too.

It lists services as:

1. Neutralize malicious activities in the cyber domain with takedown, triaging, and escalating relevant information for sectors under threats.
2. Prevent attacks by supplying reliable, actionable information (IoCs, vulnerabilities, compromised sensitive information and vulnerabilities alerting).
3. Support the medical sector and other relevant sectors with services such as incident response and technical support.
4. Act as clearinghouse for data, a connection network and a platform for facilitating those connections

There are disinformation equivalents to these:

1. Neutralize. Disinformation incident response: disinformation triage, takedown, triage and escalation.
2. Clearinghouse. Collate and share incident data, including with organizations focusing on response and counter-campaigns (the "elves" who fight the "trolls").

3. Prevent. Collate disinformation vulnerabilities and indicators of compromise (IoCs), and supply these to the organizations that we work with.
4. Support. Assess the possibility of direct attacks, and ways to be ready for that. For example, prepare resources that could be used in countering campaigns that target specific facilities, groups and high-profile individuals.

For the neutralization part, the league lists as examples:

- Infrastructures used by a threat actor that is exploiting the pandemic – malicious command and control server / DDoS servers / domains / IPs / etc.
- Exploiting legitimate services (such as open port in a legitimate website or compromised website used by hackers) and relevant to our stakeholders can be used to deploy attacks

The disinformation equivalents here would include:

- Hashtags, groups, networks, botnets, information routes, etc. used by disinformation actor groups to create and run incidents. We can map several of these ahead of time, monitor them for new events forming (e.g. qanon checkins), file abuse complaints to registrars, notify companies hosting botnets and command and control accounts, etc.
- Medical events (e.g. vaccination rollouts) that we know will trigger disinformation incidents

For prevention and support, the league lists examples:

- Alerting about vulnerabilities / compromised information and infrastructure to our stakeholders

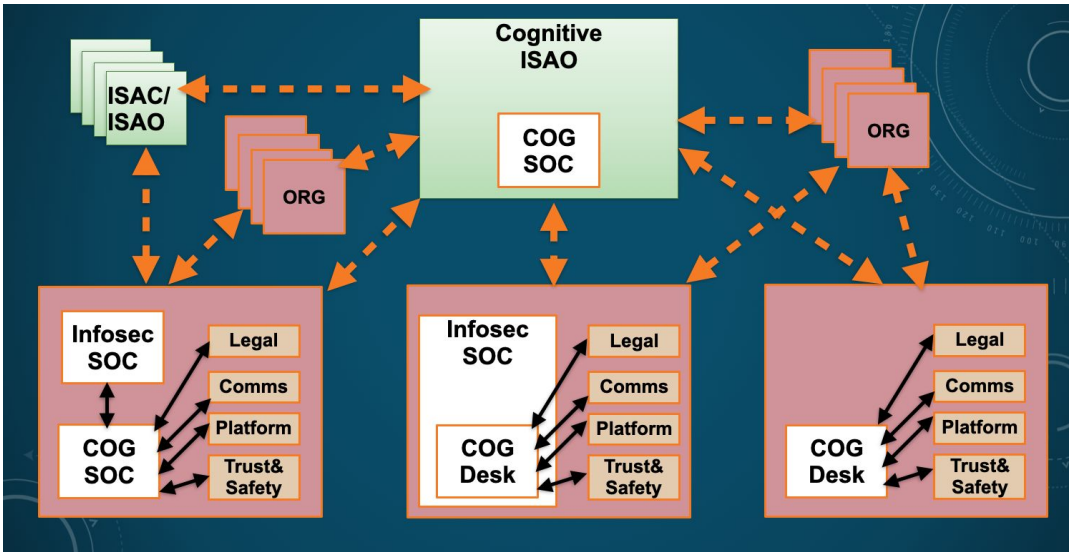
- Creating a database of malicious indicators of compromise for blocking (via both MISP and GitHub repository)
- Alerting about trends and uneventful events regarding the pandemic in the cyber domain
- Creating a database of hunting queries for alerting systems.
- Create a safe and secure infrastructure for CTI League activities
- Create reports dedicated for the stakeholders and update them about ongoing trends of attack vectors regarding their organizations, such as significant information from underground-based platforms (darknet).

This is more detailed work, but as we track more incidents and become more familiar with the methods and tools used by incident creators, some measure of prevention activities become possible.

Disinformation SOCs: Including CogSec in InfoSec

InfoSec Security Operations Centers, SOCs, are units - people, processes, technology, culture, that work on infosec operations. Most of them monitor systems, detect threats to those systems, and handle information security incidents in them.

Cognitive Security SOCs have the same function, but for disinformation and related online harms.



CogSec / InfoSec SOC configurations

There are many ways to connect a cognitive security SOC, CogSOC, to existing infosec infrastructure.

- The CogSOC