cloud security alliance®

# Cyber Threat Psychology Research Working Group


Session 2 on 24/02/2025

*Cyber Threat Psychology Working Group*

# CSA CTP Research WG: Agenda of Session on 24 Feb 2025

1. Research Project and Working Objectives (Recap), Goals and Deliverables
2. Announcement Co-Chair, Working Group Participants: New Joiners
3. Proposal & Discussion: Preparation of Streams, Stream Objectives, Stream Activities
4. Next Activities and Communication of Working Group Results

# CSA CTP Research WG: Agenda of Session on 24 Feb 2025

1. **Research Project and Working Objectives (Recap), Goals and Deliverables**
2. Announcement Co-Chair, Working Group Participants: New Joiners
3. Proposal & Discussion: Preparation of Streams, Stream Objectives, Stream Activities
4. Next Activities and Communication of Working Group Results

# CSA Cyber Threat Psychology Research: Objectives (1/3)

Research into Cyber Threat Psychology is aiming at:

1. Identifying personal conditions which foster the development of behaviours ultimately being deployed to hacktivism: shyness, genius, one-sided excellence, isolation, social media consumption, strength, …
2. Identifying social context conditions which foster the development of behaviours ultimately being deployed to hacktivism: neglect, lack of appreciation, bullying, mobbing, skills not being recognized, the power of words, social environment, political system, chance equality, …
3. Analysing the transmission mechanisms at the "supply side": most people in the same constellation don't develop the negative mindset of hackers. What are combinations of factors resulting in evil mentality?
4. Identifying potential interception points and mechanisms "supply side":
    a) Which of the above conditions and transmission mechanisms are suitable to interfere with?
    b) What possible interference patterns and approaches exist and how can these be tuned to achieve positive outcome?
    c) Longer term approaches to impact change in the conditions to prevent them from fertilising hacktivism mindset
    d) "Social engineering": target potential or actual Hackers and their social environment via the conditions and transmission mechanisms identified in this research project, to approach them and effect a mindset change

# CSA Cyber Threat Psychology Research: Objectives (2/3)

Research into Cyber Threat Psychology is aiming at (continued):

5. Analysing and identifying interception points in the transmission mechanisms between the "supply side" and the "receiver side":

   **Congruency of "supply side" and "receiver side" motivators e.g. craving for appreciation**

   a) Undermining with subversion: Get closer to the targets: intrusion into social channels, connecting, posing, praising, applauding, establishing credibility, establishing trust, collecting information, beginning to subtly seed information.

   b) Influencing with deception: working actively on the targets, leverage trust established to influence with own information which may include partial misinformation, throw baits in disguise in the context of the established trust, engage even more and foster action by the targets to reveal more critical information, etc.

   c) Acting with poisoning: "Psychology as a Weapon" and "Code as a Weapon": targeting the broad public or specific important / highly respected individuals with psychological means to poison their opinion and to leverage them thereafter as opinion leaders to achieve wide spread poisoning. Misuse the trust established and the information gathered during the undermining and influencing phases, to weaponise and intrude into protected environments via identity and authentication hijacking, misuse identity and their credibility to intrude into trusted news feeds, fora, social media to further inject and spread poisoned information to poison the receiving society.

# CSA Cyber Threat Psychology Research: Objectives (3/3)

Research into Cyber Threat Psychology is aiming at (continued):

5. Identify action points on the "receiver side":
    a) All: educate to overcome the lack of understanding of exposure to cyber attacks, social engineering, indirect exposure via careless information sharing or unconscious biases of trust, and their transmission mechanisms
    b) All: Behaviour change: how to apply curiosity and social / emotional awareness and turn it into mischievous vigilance to prevent being caught by hacking
    c) Private Individuals: awareness activities to help identifying potential persons in the personal environment who could become susceptible to developing into hacktivism, and to coach or encourage them to change mindset or route
    d) Society and Communities: How does a state's society, a community or a group respond to the communication received via the transmission channels, in particular to the subversion, deception and poisoning triade? Can this be improved, sharpened, immunised by appropriate awareness and information / education campaigns? How can state / community leadership impact and positively influence this?
    e) Corporates: Top Management culture and behaviours exemplarily demonstrated
    f) Corporates: Organisational culture change: modifying processes, incentives and organisational mindset
    g) Corporates: All staff awareness: understand the background of hacktivism as per this research project, develop novel training and real live awareness programs, apply social and emotional awareness

# CSA Cyber Threat Psychology Research: Goals, Deliverables

**What do we want to achieve and deliver:**

Research phase of the project:

- Stream by stream evolving reports which are consolidated into the overall project results in progress report
- Periodic (monthly / quarterly) presentation of interim results to CSA Global, Conferences, News, Social Media

Conclusion phase of the project:

- Project report with conclusions and proposals
- Recommendations for communication actions

Outreach phase of the project:

- Connect to communities to reach "supply side" and "receiver side"
- Actively educate communities with direct information, communication of research output re patterns, what to look for, how to approach, how to react, how to change, where to find support, etc.

# CSA CTP Research WG: Agenda of Session on 24 Feb 2025

1. Research Project and Working Objectives (Recap), Goals and Deliverables
2. **Announcement Co-Chair, Working Group Participants: New Joiners**
3. Proposal & Discussion: Preparation of Streams, Stream Objectives, Stream Activities
4. Next Activities and Communication of Working Group Results

# CSA Cyber Threat Psychology Research WG: Co-Chair

Announcement of Co-Chair: Lenka Fibikova

# CSA Cyber Threat Psychology Research WG: New Participants

## Please introduce yourselves to the group

Short Bio e.g.

- Education …
- Profession …
- Experience …
- Relevant specialisation …
- Interests related to this research project …
- Connections which could be leveraged …

# CSA CTP Research WG: Agenda of Session on 24 Feb 2025

1. Research Project and Working Objectives (Recap), Goals and Deliverables
2. Announcement Co-Chair, Working Group Participants: New Joiners
3. **Proposal & Discussion: Preparation of Streams, Stream Objectives, Stream Activities**
4. Next Activities and Communication of Working Group Results

# Cyber Threat Psychology Research: Stream Actions

**Actions from previous Working Group Call:**

- Review the proposed research streams:
  *No feedback obtained so endorsed.*
- Allocate yourselves to one or several of the proposed research streams:
  *Only few replies, alternative proposal, see next slide.*
- Communicate stream affiliation to Rolf who will set up for each stream an initial call
  *Pending / following the above action.*
- Volunteer for stream lead roles within the stream participants
  *Pending / following the above action.*
- Set up streams independently and research & discuss within the streams as a team
- Protocol within each stream discussions ("human enhanced" AI notetakers, please …)
- Streams present their progress, interim results, news, proposals, etc. fortnightly to the overall working group
- Alignment and coordination at the fortnightly overall working group calls
- Periodic presentation of interim results to CSA Global, Conferences, News and Social Media
- Target time line of completion of research project is 18 months i.e. October 2026.

# Cyber Threat Psychology Research: Streams Overview

**Research Streams:**

A. "Supply Side" Psychology

B. "Receiver Side" Psychology

C. Transmission Mechanisms

D. Communication and Interception

E. Forensics (in preparation)

# Cyber Threat Psychology Research: Stream Preparation

**Stream Preparation: Proposal**

- Little feedback obtained re participants to stream allocation choices, stream topics and approach proposed.
- Propose to:
  - Keep Working Group together over the next 6 to 8 weeks.
  - Develop a baseline document along the stream topics on the next slides, providing more detailed content and research guidance to each stream.
  - Develop an activities matrix outlining the stream-by-stream research activities and showing where combined activities (due to overlaps in the partners) are meaningful.
  - Split out into streams once the baseline document and activities outline have been done.
- Requirements to all:
  - Be active and contribute. If you cannot commit to contribute, please let the co-chairs know.
  - Contribute content: Ideas and proposals, write chapters, bring in research you are aware of, etc.
  - Reach out to your network, spread the word, actively bring in contributors with relevant expertise.
  - Make a strong effort to participate actively in all sessions over the next few months. If you cannot attend a session, please provide your inputs to the co-chairs latest on Thursday before the session, by email.

# Cyber Threat Psychology Research: Stream Content

**Topics and Activities of Research:**

A. "Supply Side" Psychology: Topics

i. Scope of "supply side actors": Prove your ego, hactivism, disgruntled employees, stalkers, financially motivated cyber crime, state-sponsored cyber warfare, cyber terrorism, …

ii. Classify the supply side actors and find historical examples for each group.

iii. Personal Conditions and Behaviour: Map out different mental and personal pathways commonly observed with actors. Identify "at-risk" personality types and behaviours evidencing these.

iv. Social Context and Behaviour: Map out different social pathways commonly observed with cyber actors. Identify "at-risk" personality types within social conditions and behaviours evidencing these.

v. Common themes how hackers rationalize their actions (moral framing, ideology, etc.)

vi. Common methods of recruiting actors (campaigns, forums, recognition, teasing and spoiling, etc.)

vii. Transmission mechanisms at the "supply side"

viii. What patterns can we identify, how and why do these work?

ix. How actors handle stress, uncertainty, law enforcement pressure, regret

x. Reintegration of actors in the society.

# Cyber Threat Psychology Research: Stream Content

**Topics and Activities of Research:**

A. "Supply Side" Psychology: Activities

i. Integration with research projects and activities in Psychological and Cyber Defence Agencies, Universities, private Research / Think Tanks

ii. Interviews with ethical hackers: learn from their motivation and their approaches

iii. Engage with HackerOne and other ethical hacking companies : deep dive into background of attacks, motivation, approaches to identify early and work on incentivising hackers to change mind / side

iv. Possible contacts to psychologists and sociologists who had contacts with actors.

v. Interviews with youth psychologists: behavioural and motivational aspects

vi. Interviews with senior psychologists analysing the information and behaviour patterns of the broader public and society

vii. Interviews with sociologists: impact from social context, environment and behaviour

viii. Interviews with behavioural scientists: understand the transmission mechanisms, ways towards mindset changes

ix. Engage with Cyber Criminologists: learn from real cases and personal situation / behaviour and context observed

x. Explore real court cases. For example, Europol publishes the cases, however, on a quite high-level basis

xi. Study of published actor interviews and information actors boast themselves with.

# Cyber Threat Psychology Research: Stream Content

**Topics and Activities of Research:**

B. "Receiver Side" Psychology: Topics

i. Scope of "receiver side actors": Individuals, communities, groups, societies, nations, corporates and institutions, all.

ii. Amplification mechanisms and influencing patterns at the "Receiver Side": What patterns can we identify, how and why do these work?

iii. How does fear of exposure impact people?

iv. How does ignorance and light-heartedness impact people?

v. Role models and trust: how do these result in people falling prey?

vi. What are common reactions of a victim?

vii. How do victims handle overt psychological distress or react if put under sublime stress?

viii. Transmission mechanisms at the "receiver side"

ix. What patterns can we identify, how and why do these work?

# Cyber Threat Psychology Research: Stream Content

**Topics and Activities of Research:**

B. "Receiver Side" Psychology: Activities

i. Integration with research projects and activities in Psychological and Cyber Defence Agencies, Universities, private Research / Think Tanks

ii. Interviews with senior psychologists analysing the information and behaviour patterns of the broader public and society

iii. Interviews with sociologists: impact from social context, environment and behaviour

iv. Interviews with behavioural scientists: understand the transmission mechanisms, ways towards mindset changes

v. Engage with SOCs of corporates and institutions, the SOC Working Group of SIGS, CSA, similar: Receiving Side Patterns

vi. Engage with Pen Testing Companies: Corporate Behaviour in response to pen test results

vii. Engage with CISOs and CEOs: Corporate Behaviour, Corporate Culture, actively living and demonstrating exemplary behaviour of vigilance based on understanding the emotional and mindset background of hacktivism

viii. Engage with Cyber Criminologists: learn from real cases and personal situation / behaviour and context observed

# Cyber Threat Psychology Research: Stream Content

**Topics and Activities of Research:**

C. Transmission Mechanisms: Topics

i. Transmission mechanisms between the "supply side" and the "receiver side".

ii. Why do these transmissions work, which patterns can we derive?

iii. Analyse the "subversion – deception – poisoning" triad

iv. Congruency of "supply side" and "receiver side" motivators e.g. craving for appreciation

v. Methods used in phishing and social engineering. Known techniques to deal with those.

vi. Cognitive biases exploited by the supply side. Known techniques to deal with the biases.

vii. Rhetoric used in the transmission (e.g., fear, reward).

viii. Use of social media and other public platforms.

ix. Impact of AI on the transmission.

# Cyber Threat Psychology Research: Stream Content

**Topics and Activities of Research:**

C. Transmission Mechanisms: Activities

i. Integration with research projects and activities in Psychological and Cyber Defence Agencies, Universities, private Research / Think Tanks

ii. Interviews with ethical hackers: learn from their experience on how transmission works

iii. Engage with HackerOne and other ethical hacking companies : deep dive into how attacks transmit

iv. Interviews with psychologists and behavioural scientists about the subversion – deception – poisoning transmission mechanisms and patterns, and to identify approaches to effect mindset changes to interrupt the transmission.

v. Interviews with senior psychologists analysing the information and behaviour patterns of the broader public and society

vi. Engage with SOCs of corporates and institutions, the SOC Working Group of SIGS, CSA, similar: Receiving Side Patterns

vii. Engage with Pen Testing Companies: Corporate Behaviour in response to pen test results

viii. Engage with CISOs and CEOs: Corporate Behaviour, Corporate Culture, actively living and demonstrating exemplary behaviour of vigilance based on understanding the emotional and mindset background of hacktivism

ix. Engage with Cyber Criminologists: learn from real cases and personal situation / behaviour and context observed

# Cyber Threat Psychology Research: Stream Content

**Topics and Activities of Research:**

D. Communication and Interception: Topics

i. Interception at "Supply Side": possibly split into Hackers, Environment

ii. Behavioural Change at "Receiver Side": possibly split into All, Corporates, Institutions, Privates

iii. How can communication modify the "Receiver Side" behaviours: boasting, careless information sharing, unconscious biases of trust

iv. How to establish and nurture curiosity and social / emotional awareness and turn it into mischievous vigilance?

v. Effective mass communication and immunisation

# Cyber Threat Psychology Research: Stream Content

**Topics and Activities of Research:**

D. Communication and Interception: Activities

i. Integration with research projects and activities in Psychological and Cyber Defence Agencies, Universities, private Research / Think Tanks.

ii. Interact with media and communication specialists: how to disseminate the messages so that the right target audience can be reached and the message comes across in an encouraging and change enticing way?

iii. Interviews with ethical hackers: learn from what they would have reacted to / listened to.

iv. Interviews with youth psychologists: how to approach the supply side addressing the behavioural and motivational aspects which should be recognised and changed?

v. Interviews with senior psychologists how to modify the information and behaviour patterns of the broader public and society

vi. Interviews with behavioural scientists: understand the transmission mechanisms, ways towards mindset changes

vii. Engage with CISOs and CEOs: Corporate Behaviour, Corporate Culture, actively living and demonstrating exemplary behaviour of vigilance based on understanding the emotional and mindset background of hacktivism

viii. Engage with Cyber Criminologists: learn from real cases and personal situation / behaviour and context observed

# Cyber Threat Psychology Research: Stream Activities Matrix

## Draft / Initial Proposal of overlay for combined stream interviews:

| Interviewee | Stream A: Supply Side | Stream B: Receiver Side | Stream C: Transmission | Stream D: Communication | Stream E. Forensics |
|---|---|---|---|---|---|
| **External research projects** | x | X | X | X | X |
| **Ethical hackers** | motivation and approaches | - | experience how transmission works | | tbd |
| **Ethical hacker companies** | background, motivation, approaches | - | deep dive how attacks transmit | what would they have reacted to | tbd |
| **Psychologists** | contact to actors<br>behaviour, motivation | behaviour patterns of the broader public and society | subversion-deception-poisoning appraoches to interrupt transmission;<br>behaviour patterns | how to approach supply side to address behavioural and motivation aspects;<br>how to modify info and behaviour patterns | tbd |
| **Sociologists** | contact to actors<br>social context, environment, behaviour | social context, environment, behaviour | subversion-deception-poisoning appraoches to interrupt transmission | | tbd |
| **Behavioural scientists** | transmission mechanisms, ways towards mindset changes | - | - | understand the transmission mechanism | tbd |
| **Cyber criminologist** | real cases, behaviours | real cases, behaviours | real cases | real cases | tbd |
| **SOCs, SIGS SOC WG, other SOC WGs** | - | receiving side patterns | receiving side patterns | - | tbd |
| **Pentesting companies** | - | corporate behaviour to pentest results | corporate behaviour to pentest results | - | tbd |
| **CISOs and CEOs** | - | corporate behaviour, culture | corporate behaviour, culture | corporate behaviour, culture | tbd |
| **Media and comm. specialists** | - | - | - | info dissemination approaches | tbd |

# CSA CTP Research WG: Agenda of Session on 24 Feb 2025

1. Research Project and Working Objectives (Recap), Goals and Deliverables
2. Announcement Co-Chair, Working Group Participants: New Joiners
3. Proposal & Discussion: Preparation of Streams, Stream Objectives, Stream Activities
4. **Next Activities and Communication of Working Group Results**

# What's next

## Proposed Next Steps:

- All: Reach out to your network and identify potential contributors to this research working group, feedback to Rolf & Lenka / co-chairs, arrange for introduction calls.
- ~~Rolf: identify co-chair and propose to working group at next session.~~ *Done*
- Rolf & Linda: set up shared Teams channel, with files area, with participants added as users.
- Rolf & Lenka / co-chairs: Define Charter of Cyber Threat Psychology Research Working Group, submit to working group for review, with formal endorsement by working group and CSA.
- ~~Rolf: & tbd / co-chair: Set up fortnightly Working Group calls.~~ *Done*
- ~~Stream Leads: constitute streams, set up weekly stream calls, initiate research activities.~~ *Replaced by new proposal below*
- As per new proposal:
  - All: Keep Working Group together over the next 6 to 8 weeks.
  - All: Develop a baseline document along the stream topics on the next slides, providing more detailed content and research guidance to each stream.
  - All: Develop an activities matrix outlining the stream-by-stream research activities and showing where combined activities (due to overlaps in the partners) are meaningful.
  - Split out into streams once the baseline document and activities outline have been done.

# What's next

## Proposed Next Steps:

- ~~All: contribute within streams re research, literature, connections, …~~ *Replaced by new proposal below*
- As per new proposal:
  - All: Be active and contribute. If you cannot commit to contribute, please let the co-chairs know.
  - All: Contribute content: Ideas and proposals, write chapters, bring in research you are aware of, etc.
  - All: Reach out to your network, spread the word, actively bring in contributors with relevant expertise.
  - All: Make a strong effort to participate actively in all sessions over the next few months. If you cannot attend a session, please provide your inputs to the co-chairs latest on Thursday before the session, by email.
- Rolf & Lenka / co-chairs, Stream Leads: outline research project time line and deliverables and integrate into Charter.
- Rolf, Stream Leads, all stream participants: Prepare news release for CSA Swiss Chapter Website, LinkedIn channel, CSA Global, and at upcoming events.
- Rolf, Stream Leads, all stream participants: Monthly news updates to above channels.