cloud security alliance®

Cyber Threat Psychology Research Working Group

Session 1 on 10/02/2025

Cyber Threat Psychology Working Group

CSA CTP Research WG: Agenda of Session on 10 Feb 2025

1. **Introduction: Research Project and Working Objectives**
2. **Introduction: Working Group Participants**
3. **Proposal and Discussion: Streams, Approach and Activities**
4. **Time Line, Next Steps and Logistics**

CSA CTP Research WG: Agenda of Session on 10 Feb 2025

1. **Introduction: Research Project and Working Objectives**
2. Introduction: Working Group Participants
3. Proposal and Discussion: Streams, Approach and Activities
4. Time Line, Next Steps and Logistics

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 CTP Research WG: Agenda of Session on 10 Feb 2025

1. Introduction: Research Project and Working Objectives
2. **Introduction: Working Group Participants**
3. Proposal and Discussion: Streams, Approach and Activities
4. Time Line, Next Steps and Logistics

CSA Cyber Threat Psychology Research WG: 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 10 Feb 2025

1. Introduction: Research Project and Working Objectives
2. Introduction: Working Group Participants
3. **Proposal and Discussion: Streams, Approach and Activities**
4. Time Line, Next Steps and Logistics

Cyber Threat Psychology Research: Structure Proposal (1/4)

Proposed Research Streams:

A. "Supply Side" Psychology
   i. Personal Conditions and Behaviour
   ii. Social Context and Behaviour
   iii. Transmission mechanisms at the "Supply Side"
   iv. What patterns can we identify, how and why do these work?

B. "Receiver Side" Psychology
   i. All
   ii. Individuals
   iii. Communities, groups, societies
   iv. Corporates and institutions
   v. Amplification mechanisms and influencing patterns at the "Receiver Side": What patterns can we identify, how and why do these work?

Cyber Threat Psychology Research: Structure Proposal (2/4)

Proposed Research Streams:

C. Transmission Mechanisms

   i. Transmission mechanisms between the "Supply Side" and the "Receiver Side"

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

D. Communication and Interception:

   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: Structure Proposal (3/4)

Proposed Approach:

- Review the proposed research streams
- Allocate yourselves to one or several of the proposed research streams
- Communicate stream affiliation to Rolf who will set up for each stream an initial call
- Volunteer for stream lead roles within the stream participants
- 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: Structure Proposal (4/4)

Proposed Activities:

- Integration with research projects and activities in Psychological and Cyber Defence Agencies, Universities, private Research / Think Tanks
- Interviews with ethical hackers: learn from their motivation and their approaches
- 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
- Interviews with youth psychologists: behavioural and motivational aspects
- Interviews with senior psychologists analysing the information and behaviour patterns of the broader public and society
- Interviews with sociologists: impact from social context, environment and behaviour
- Interviews with behavioural scientists: understand the transmission mechanisms, ways towards mindset changes
- Engage with SOC Working Group of SIGS: Receiving Side Patterns
- Engage with Pen Testing Companies: Corporate Behaviour in response to pen test results
- 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
- Engage with Cyber Criminologists: learn from real cases and personal situation / behaviour and context observed

CSA CTP Research WG: Agenda of Session on 10 Feb 2025

1. Introduction: Research Project and Working Objectives
2. Introduction: Working Group Participants
3. Proposal and Discussion: Streams, Approach and Activities
4. **Time Line, Next Steps and Logistics**

What's next

Proposed Next Steps:

- All: Reach out to your network and identify potential contributors to this research working group, feedback to Rolf & tbd / co-chair, arrange for introduction calls.
- Rolf: identify co-chair and propose to working group at next session.
- Rolf & Linda: set up shared Teams channel, with files area, with participants added as users.
- Rolf & tbd / co-chair: 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.
- Stream Leads: constitute streams, set up weekly stream calls, initiate research activities.
- All: contribute within streams re research, literature, connections, …
- Rolf & tbd / co-chair, 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.