UNPACKING THE TECH-SECURITY DRIVES; PROTECTING CIVIC SPACE

CT & tech workshop summary notes - 27 and 28 June 2023

A. Fintech / Tech CFT profiling

Is using fintech effective – does it work?

- benefits of tech for CSOs - can we find research on this?
- effectiveness – how much is fintech effective - unclear
- disproportionate negative impact on very few people or organisations

Data usage

- data collection relies on many sources, including publicly available sources
- is data tampered with – additional needed question!
- problem for e.g. Palestinian groups when taking data from public sources, due to smear campaigns online against those groups – trying to work with banks to recognise and understand online public info is biased or false

Transparency issues

- how sure developers are that they account for all mistakes are those only ones, if the system is untransparent?
- reasons for not sharing information – 'bad actors will exploit vulnerabilities'; IP violations; national security issues
- are there any requirements for finance sector to produce some transparency reports? Currently no

Regulation that could apply

- any regulation that applies to fintech? No specific ones, other than data protection. Upcoming AI regulation - will EU AI regulation apply to fintech developers? Possibly
- did anyone try to challenge the fintech tool via GDPR rules? Based on data collection / retention, etc. – can it be utilised? Not fully clear
- consumers rights legislation, is it applicable? Possibly
- where and to whom can we address FOIA requests, to avoid private sector refusal? need to understand and discuss with FOIA experts on a) whom to address, b) what can we ask for

CSOs at the table (not on the menu)

- need to put CSOs at the table for discussions when designing and developing tech solutions
- CSOs don't have resources and capacity to participate in developing tech – but we can show evidence of harm, raise grievances, collect evidence on financial exclusion, more data we have better we can talk to governments and other stakeholders about this. Find patterns, etc.
- financial exclusion creates risks and many governments want to fix this
- standards setters and policy makers need to take more proactive role to convene and take into account these issues when developing technology

Additional evidence and harm mapping

- more sharing and dissemination of evidence is needed on problems and issues
- develop fintech AML/CFT playbook, typologies of harm and mitigating measures for developers

Pathways for advocacy / actions:

- Framing the issue as financial inclusion!
- Focus of CSOs should be on transparency, awareness raising, legal challenges towards technology use

1. National level study – mapping

- more evidence needed
- specific impact on marginalised groups

2. Develop brief playbook of CSO concerns

- offered to banks, developers
- initiating dialogue on national level + big banks ("mother" institutions)
- connect with dialogue initiatives on global level, e.g. with FATF + banks
- connect with current de-risking / financial exclusion tracks of discussions (additional form of de-risking + profiling)

3. Tech design workshops

- for banks? Developers
- need to explore possible avenues

4. Regulative push back

- utilising FOIA → exploration needed
- utilising GDPR and other data privacy rules → exploration for redress needed
- other regulation (upcoming) → use as advocacy leverage

B. goFintel strategy plan

Presentation by OCT team:

- it is promoted as "the new, best, tool" for AML/CFT purposes
- development should finish end 2023 (tbc)
- goal – help member states address challenges from UN Security Council Resolution 2462
- data collection, ingestion and storing in real time or batch processing
- data quality checks performed
- data is consolidated
- data can be automatically screened - using any lists available
- data retention rule – member states can configure according to their legislation (only if exists)
- operational and strategic analysis, correlating transaction reports with data from multiple sources (not identified which sources - using data from crypto, social security numbers, SRTs, IP address…)
    - the UN does not have access to data processed in goFintel
- member states have control what type of data to ingest
- range and scope of data can be international, national, regional depending on regulation in country

- previous promo video included using and scraping data from "publicly available sources" which typically means also social networks, internet at large
- modular architecture – contribute to platform by user community
- flexible tool
- python code
- rule based system – replacing all manual work by analysts (screening sanction lists, analytical work, etc.) – member states can configure their own rules
- users – financial intelligence units of member states, hope to expand beyond FIUs, to law enforcement
- developer team builds a "house" - member states can define their own modules, their own data input, own menu structure, customise different processes and exports, e.g. export for police (data allowed to see by police, not all data);
- still no case management component included but should have customised work flows
- there will be community of users sharing best practices
- beta version was tested by Dutch government - satisfying for analysis
- first version expected in Summer 2023
- deployment to NL might be test phase before human rights due diligence is completed, but all due diligence should be done before tool goes live, by end 2023
- intention is to be guided by human rights principles
- engaging human rights consultant (from Summer 2023!) to ensure these aspects will be taken into account

Discussion and answers to questions by the Hub members:

- UN OCT will launch consultative process to explore ways in which goFintel should approach human rights due diligence in line with human rights and UN policies and guidance, as well as human rights due diligence in tech development (by OHCHR)
- in order for member states to use tool, in line with international standards, UN wants to make sure member state has legal, policy and operational framework with adequate safeguards against abuse – they are different ways to use tool, need insurance that tool will be in line with international law including human rights
- there will be user agreements with member state – to use in responsible way e.g. only if there is adequate legislation in place
- part of pre-deployment assessment if MS has prerequisite (legal, operational, regulatory framework) to ensure proper operations / including storage
- initial compliance check for member state on regulation and structure – likely conducted by UN CTED. UN CTED will make these assessments, they will count on civil society for information. UN CTED will assess gaps in CT framework, in early stages when state expresses interest – ensure to gather all info on implementing CT framework.
- UN Special Rapporteur(s) could be a part of consultative process for human rights issues (?)
- The tool comes as part of broader package, with set of criteria to fulfill, existence of proper legal, policy, operational framework, with safeguards – are they public? Developing the criteria now, with consultant to include during consultation, it should be publicly available
- only those member states with criteria will get it
- member states need to ask for tool, then initiate the process
- member states will need to pay for it - how much – they did not respond
- license agreement for member state to make sure system works well – but how to keep track of errors / mitigate those

- constant patches being deployed
- team will immediately address problems and send out a patch for performance issue
- different issues possible – system issue, member state environment etc.
- auditing aspect and leverage to member state : continuous engagement required, to request patches and improvements
- every user system will be logged for auditing – recordings of all steps.
- initial license cannot be revoked for member state, only updates and improvements
- not clear how to prevent abuse
- UN would have a residual responsibility for as long as member state is using the tool – currently exploring (not clear fully) – how to actually deal with continuous due diligence policy and how to embed monitoring with some human rights parameters
- only flagged (suspicious) transactions will be included in system (but calibrated by member states)
- flagged by CSOs – potential abuse of SRTs and red flags in specific member states for specific groups / customers (there will be inconsistency in approach)
- human rights impact assessment should be part of process – to come, plus, country specific assessments when there is requests

Inconsistent claims:

- Stage of tool development / piloting and possibility for meaningful input – is there enough time for HRDD and consultation with CSOs, by end 2023?
- Will human rights impact assessment be made public and can CSOs provide feedback?
- CTED role in measuring compliance: not clear e.g. to what degree CTED implements input from CSOs into their assessment esp. concerns about human rights. Can CTED present a full picture of human rights issues – supporting idea for involving UN SRs in consultation, and CSOs in consultation / assessments.

Unanswered questions:

- How can scraped data from social media be incorporated in this tool?
- Will the public know which countries use the tool?
- MS license agreement – is there obligation on confidentiality for the tool – transparency issues, auditing from academia, CSOs...?
- If UN has no access to data, and member state access is segmented, what auditing and oversight is in place to make sure tool operates reliably?

Action plan and next steps:

Disrupt and engage = dual strategy depending on the responses and possibilities for action

In general:

- Request follow up meeting with broader group of CSOs (incl from two global coalition on FATF and UN/CT)
- obtain more internal info
- collect further questions by Hub members (and others)
- Develop stakeholder analysis of who can be supporter to the process, and create broader coalition.

Engage:

- Call for HRIA + Due diligence processes

- Research other tools – goTravel, French similar tool
- Discuss with OHCHR and SR positions and coordination on this
- put together list of asks / demands
- consult experts to develop draft criteria for what information can be shared and how much– what to do in case of abuse (by governments?) – input to process elements for tool use
- identify IT experts who can help with further understanding of tool

Concrete suggestions and asks:

- prepare proposal for accountability over use of tool (e.g., UN OCT to make guidance for national human rights institutions and other institutions on how to monitor safeguards for human rights while government is using tool)
- talk to banks how to formulate SRTs asks – only flagged transactions included in system (but calibrated by MS) - potential abuse of SRTs and red flags in specific MS for specific customers – work with UN OCT how to mitigate this
- create advisory body including CSOs on UN level to advise / monitor the overall use of systems – UN OCT open to potential role of CSOs, to identify safeguards, criteria and right measures

National level action

- identify and engage with key target governments / democratic
    - Netherlands, Germany

Monitor implementation:

- Monitoring design
- Accountability,
- Engage mechanisms

Disrupt:

- CSOs to consider developing shadow report + risk analysis once information is collected
- Involve National HR Commission
- Who from EU can be concerned about privacy issues
- Create connections with those concerned about goTravel
- Involve banks

C. Surveillance response pathways

1. **Policy advocacy track– national legislation**: calling for surveillance ban and push backs on exemptions (e.g. national security, CT, emergency powers, law enforcement)

Potential actions include:

- creating blueprints for CSO national level push back cases (Canada, Brazil, EU…)
- country cases / examples of litigating or challenging regulation, anonymised - see e.g. in this report.

2. Policy advocacy track - global level

Potential actions include:

- continue advocacy at UN level and other relevant fora

- exploring innovative narratives against normalisation of surveillance – campaigning, utilising media / journalists to bring in civic space angles

3. Linking advocacy efforts to capacity building, especially for non-digital rights organizations

Potential actions include:

- team up national level CSOs digital + non digital organisations for evidence collection and additional strategising on concrete steps

4. Exploring strategic litigations options

Potential actions include:

- e.g. suing a company exporting facial recognition technology from France to Egypt that is deployed against protests
- established court cases: see e.g. in this report.

Example of national level intervention and assistance - Mexico

- team up civic space CSOs + digital CSOs into coordination for:
    a. additional evidence gathering supported by digital expertise to expose specific harms to CSOs
    b. strengthen and develop new national advocacy steps / options and have it linked with their work - includes strategic litigation; advocacy on regulation, etc.
    c. create blueprints for sharing cross-regions and for regional and global advocacy level where CSOs can provide examples

D. Content moderation response pathways

1. Policy advocacy track - national regulations including content moderation guidance or soft law

Potential actions include:

- help to unpack copycat EU Digital Services Act and TERREG regulation to support national CSOs in pushing back with arguments (e.g. in Mexico, Turkey..)
- creating blueprints for CSO national level push back cases

2. Linking advocacy efforts to capacity building, especially for non-digital rights organizations

Potential actions include:

- help make further connections national level CSOs digital + non digital organisations for evidence collection and additional strategising on concrete steps

3. Exploring strategic litigations options

Potential actions include:

- e.g. French content moderation CT case, based on TERREG
- ad hoc providing civic space perspective in specific cases (e.g. Meta Oversight Board submission)

E. Notes from survey

Participants can offer the following specific expertise and insights related to the topic – please ask to be paired up or reach out directly to colleagues via Expert Hub platform:

1. BCNL: Involved in drafting the first Sectoral TF Risk Assessment for NPOs in Bulgaria.

2. Expertise on CTF, new technologies, and weaponisation of FATF standards against regime threats.
3. Expertise on FATF and international-level anti-financial crime architecture.
4. Ukrainian experience with digital tools for checking connections to terrorism and sanctions.
5. Efforts within the Cyprus context on counter-terrorism and anti-money laundering, including coalition-building with authorities and CSOs.
6. Experience on surveillance and its impact within the Asian context, particularly related to emergency legislation.
7. Experience in advocacy around surveillance and biometric technologies, litigation processes in Mexico and internationally, and sharing position papers and reflections on regulation and moratorium.
8. Experiences in Malawi on countering threats to civic space and pushing back against them.
9. Insights from German CSOs on development cooperation and humanitarian assistance debates.
10. Practical experience in campaigning against biometric mass surveillance.
11. Knowledge and insights on the use of technology and its impact on human rights, including research on the prosecution of terrorism-related content on social media platforms.
12. Extensive work on CFT, AML, and R8 in North Macedonia, with experience sharing on national, regional, and international levels.
13. Gathering information and knowledge on counter-terrorism legislation and practice in the Western Balkan region.
14. Expertise on civic engagement, freedom of association, and protecting civic space, with a focus on strategies for mobilising communities and fostering inclusive participation in counter-terrorism efforts.
15. Experience in research and action on countering state vigilantism and the asymmetry between the private sector and civil society.
16. Extensive work on countering terrorist financing, systemic racism/rights violations in Canada, and activities related to biometrics, national security, and content moderation laws.
17. Focus on utilising technology in countering terrorism, creating counter-terrorist narratives in cyberspace, and the impact of terrorist networks using digital platforms.
18. Identification of risks related to surveillance technologies and recommendations to states.
19. Monitoring developments at the UN regarding regulations/guidance related to terrorism and technology.
20. Expertise on the digital rights impacts of counter-terrorism measures.
21. Experience in Uganda related to counter-terrorism.
22. Experience in drafting the Bulgarian Sectoral Risk CFT Assessment for NPOs.
23. Malawian experience with relevant laws and policies for countering terrorism.
24. Feedback from advocating human rights in France.
25. Expertise in financial access, counter-terrorism, and human rights, working with civil society and human rights defenders.
26. Civic space and advocacy experience in Tanzania.