Project craaft

# Terrorism Financing & New Technologies

Stephen Reimer, Sr. Research Fellow, RUSI
27 June 2023

**www.projectCRAAFT.eu**

Collaboration, Research & Analysis Against the Financing of Terrorism

This project was funded by the European Union's Internal Security Fund – Police


United Nations Security Council
Counter-Terrorism Committee
UN Security Council
Counter - Terrorism Committee
Special Meeting on
Countering the Use of New and Emerging
Technologies for Terrorist Purposes
29 October 2022
DELHI - INDIA
United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)
SPECIAL MEETING
Countering the Use of New and Emerging
Technologies for Terrorist Purposes
28 OCTOBER 2022 - MUMBAI
29 OCTOBER 2022 - DELHI
Hosted by the Ministry of External Affairs,
Government of India


United Nations Security Council
Counter-Terrorism Committee
UN Security Council
Counter - Terrorism Committee
Special Meeting on
Countering the Use of New and Emerging
Technologies for Terrorist Purposes
29 October 2022
DELHI - INDIA
Hosted by the Ministry of External Affairs
28


Let’s all just calm down...
United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)
SPECIAL MEETING
Countering the Use of New and Emerging Technologies for Terrorist Purposes
28 OCTOBER 2022 - MUMBAI
29 OCTOBER 2022 - DELHI
Hosted by the Ministry of External Affairs, Government of India
United Nations Security Council
Counter-Terrorism Committee
UN Security Council
Counter - Terrorism Committee
Special Meeting on
Countering the Use of New and Emerging Technologies for Terrorist Purposes
29 October 2022
DELHI - INDIA
Hosted by the Ministry of External Affairs
CHAIR
28


RUSI
EUROPE
Project
craaft
Collaboration, Research & Analysis
Against the Financing of Terrorism
Occasional Paper
Bit by Bit
Impacts of New Technologies on Terrorism
Financing Risks
Stephen Reimer and Matthew Redhead


*Why study TF & New Tech?*

- EU policymaking
- Speed, efficiency, UX
- Vulnerabilities v. Sceptics
- What degree of threat?
- Crafting CTF responses

# Methodology

- “New Tech”: FinTech, crowdfunding, virtual assets, social media
- Operational & Organisational TF
- 25 expert consultations
- 212 attacks (Jan ’15 – Nov ‘21)
- 49 organisational financing cases

# Potential TF Impacts (Myths)

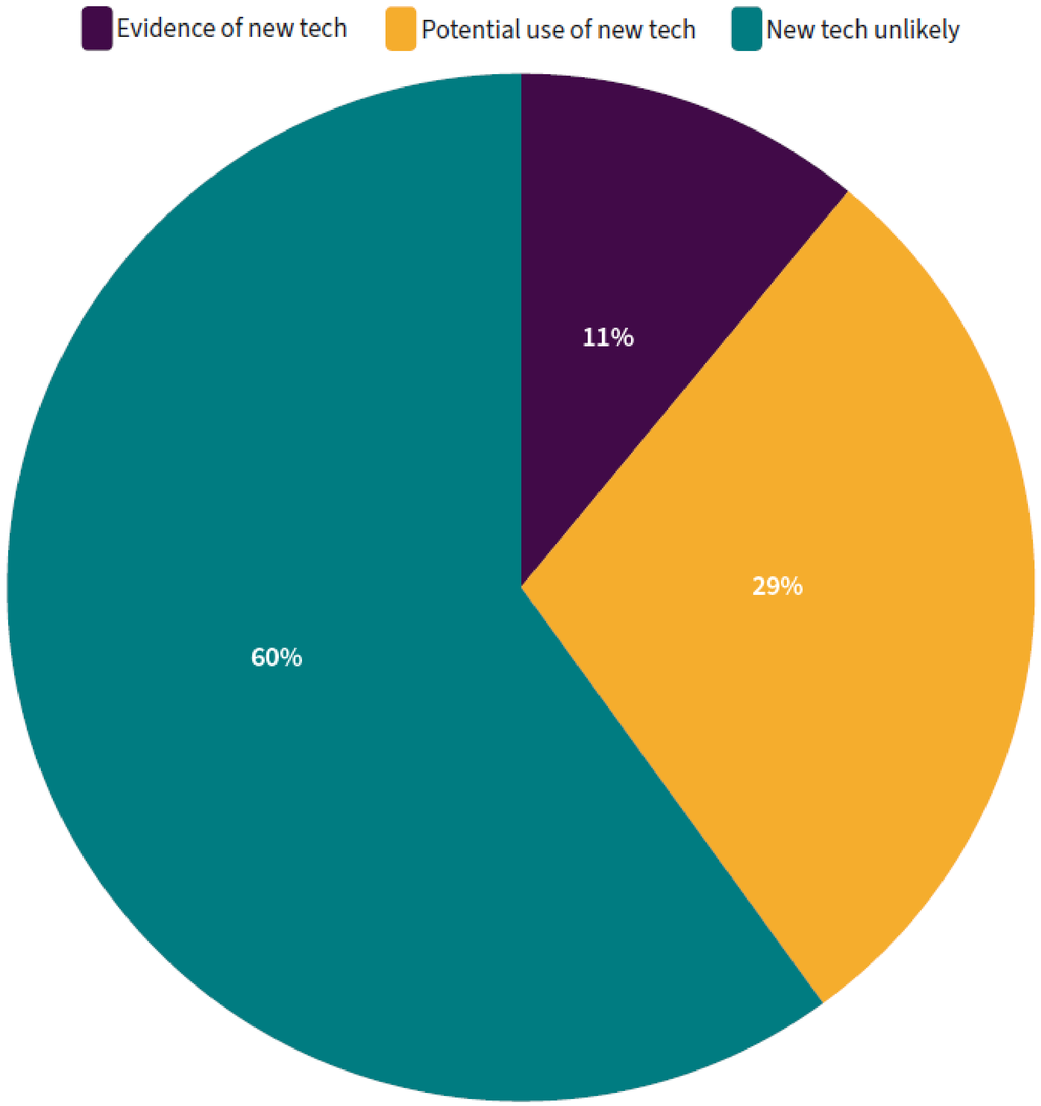
- Offering new channels (e.g. crowdfunding on social media)
- Support TF tradecraft (e.g. virtual assets as supposedly anonymous)
- Reduced surveillance (e.g. assumed weaker fin crime controls at FinTechs)

# Key Findings

- *No transformational effect of new tech on TF in Europe*
- Operational financing: little use, virtually no VAs, but some 1st generation payments providers
- Organisational financing: more use, but tried-and-tested methods prevail, sometimes in tandem with new tech

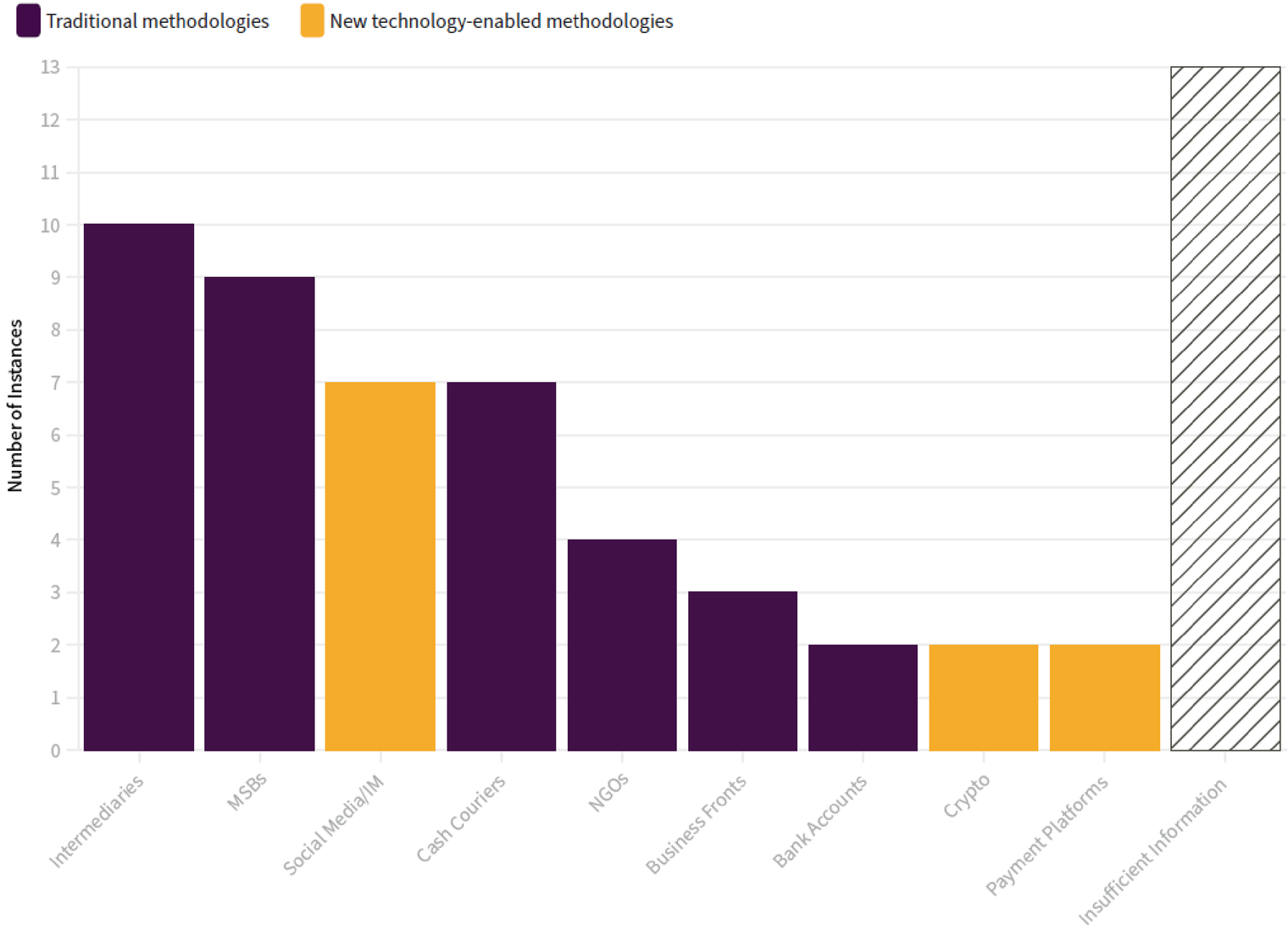
# Operational Financing

- Useful material in 65 of 212 cases on financing means
- Darknet purchases of attack components with VAs (Sonboly, DE, 2016; Bishop, UK, 2018)
- Online payments services: PayPal (Rehman, UK, 2015; Ahmed, UK, 2019) and Payoneer ("Lyon Bomber", FR, 2019)
- Why not VAs?: public ledger, technological know-how, limited use on surface web, lack of necessity



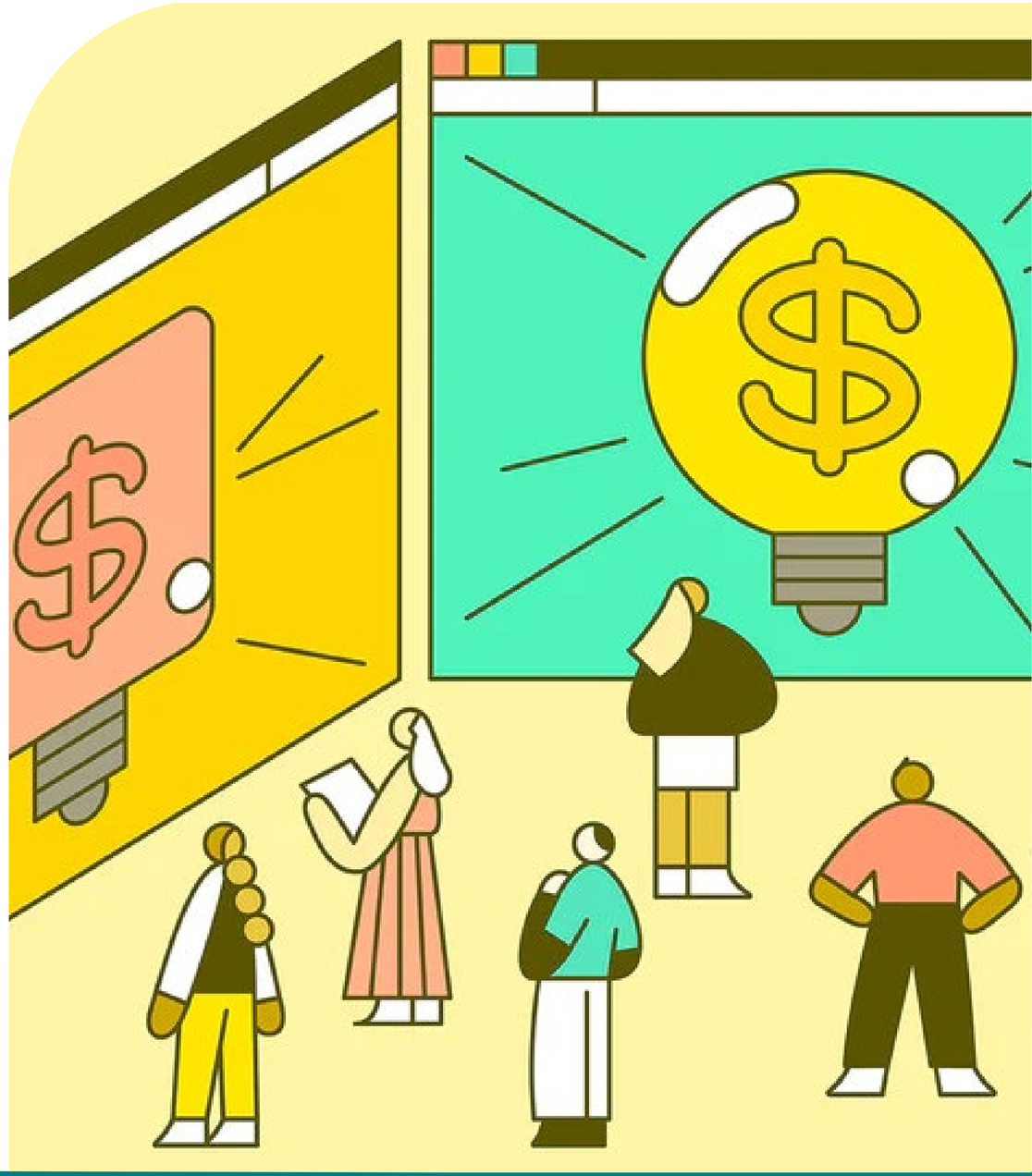
# Org Financing

- Groups promoting VAs, but enforcement action has increased in-step (Hamas announcement: “no further Bitcoin donations please”)
- “Payments services appearing with greater regularity”, but still limited relative to traditional methods
- Social Media: donation seeking tends to be carried out under charitable pretence (“Justice for Sisters” via PayPal MoneyPools)



# Crowdfunding & Charity

- “Your Sister in the Camp” via Telegram, arrests in Germany
- Donation-based platforms versus “pop-up” campaigns on social media
- #EndSARs (Nigeria) – online crowdfunding disrupted via CTF intervention
- Move towards tighter regulation… another victim of the “Vulnerabilities” approach?

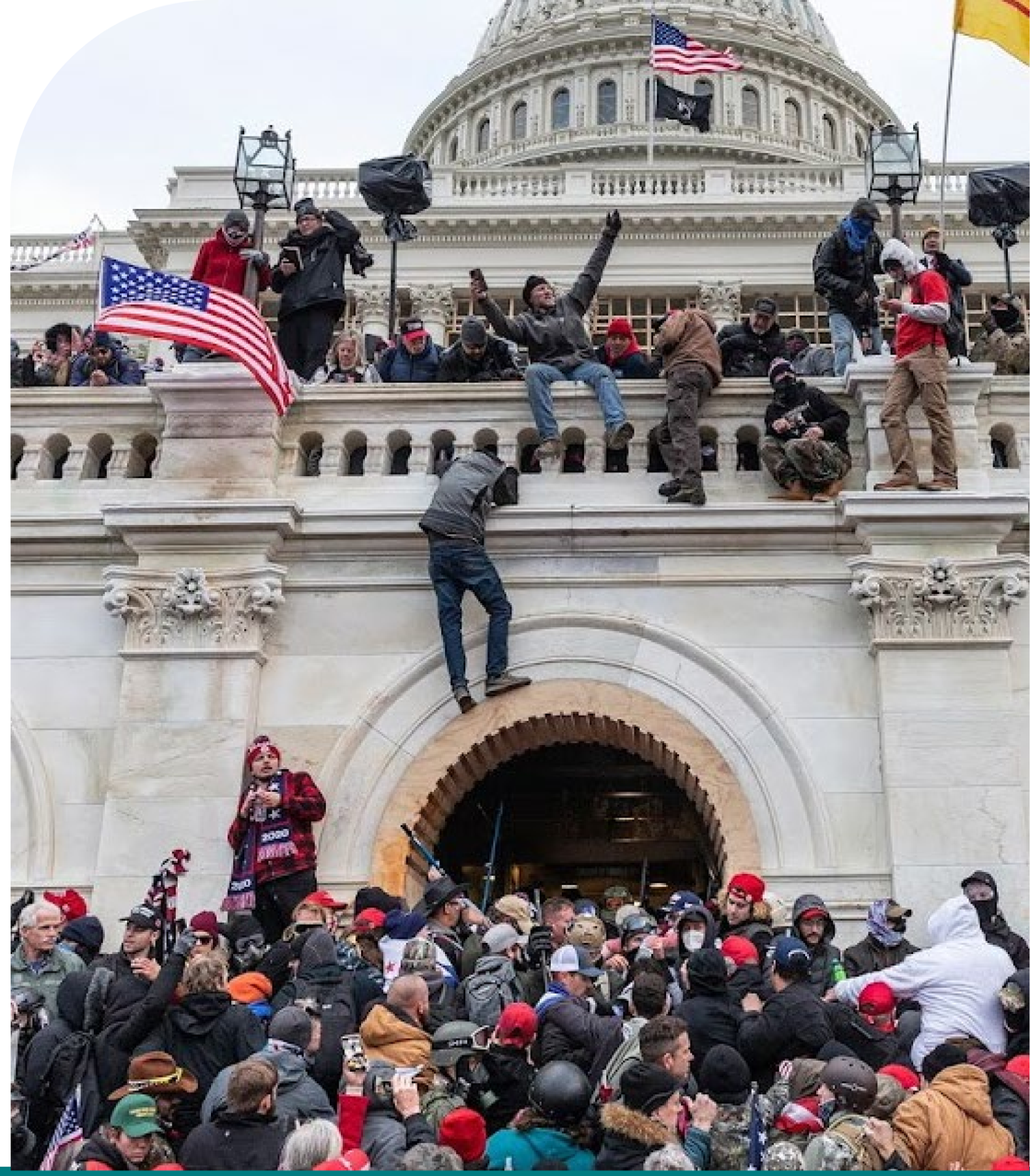


# Responses: Public Sector

- Virtual assets, cryptocurrency & their service providers often seen as the “riskiest new tech for TF”
- FinTech replicating traditional financial services subsumed under existing AML/CTF… without calibrating to sub-sector risk
- Social Media under no CTF obligations (AMLD or Terrorist Content regulation)

# Responses: Private Sector

- Concern with regulatory and reputational risk
- De-platforming, de-risking, avoidance – far-right crowdfunding campaigns removed, followed by payments providers withholding services
- These strategies give FinTech and other new tech firms ample say in who can/can't access their financial services.



# Some Recommendations

1. European Banking Authority should produce FATF-style sector-focused guidance on applying the risk-based approach to different FinTech subsectors

2. National FIUs should enter into dialogue with FinTech sector to establish partnership for data-sharing as part of suspicious activity reporting

3. EFIPPP should bring in leading FinTechs to better inform the work of supervisors and Europol, so they can offer better regulatory guidance and collect intelligence on TF risk

BL 1 – Be adaptable: threat picture likely to change particularly with wider societal use of different new technologies

BL 2 – Lots of bad regulation of new financial tech is based on myths of TF risk