

Understand the Dimensions of Organised Crime and Terrorist Networks for Developing Effective and Efficient Security Solutions for First-line-practitioners and Professionals

9TH CoU ON SAFE, SECURE AND RESILIENT SOCIETIES - WORKSHOP ON CYBERCRIME

TAKEDOWN

Identify . Prevent . Respond



Horizon 2020
Research and Innovation Action
FCT-16-2015
Project number: 700688

Brussels, BE
December 6, 2017



1) TAKEDOWN Project Overview

2) **“First Insights from the Empirical Research”**: What do the LEAs and other players (such as first-line-practitioners) identify as major challenges and requirements?

3) **“Modelling the Pathways and Trajectories of Organized (Cyber) Crime and Terrorism”**: How can we get to a better understanding of (organized) cybercrime and terrorist networks BEFORE we develop technological solutions? (approaching the topic through the analytical TAKEDOWN Model)

4) Outlook

1) TAKEDOWN Project Overview

OBJECTIVES

O1 **ANALYSE** the body of scientific **knowledge** as well as existing **models**

O2 **UNDERSTAND** the **processes** that lead to OC/TN and their impacts

O3 **DEVELOP** a multi-dimensional **model** for both OC and TN

O4 **CREATE** a set of practitioners' **toolkits** and **policy recommendations**

O5 **BUILD** a web based **Open Information Hub** with public service modules

O6 **DEVELOP** a modular **Solutions Platform** for LEAs and professionals

O7 **LEVERAGE** the **collaboration** between the relevant stakeholders

ACTIVITIES

<= **Desk Research and Analysis**

<= **Empirical Research**

<= **Conception**

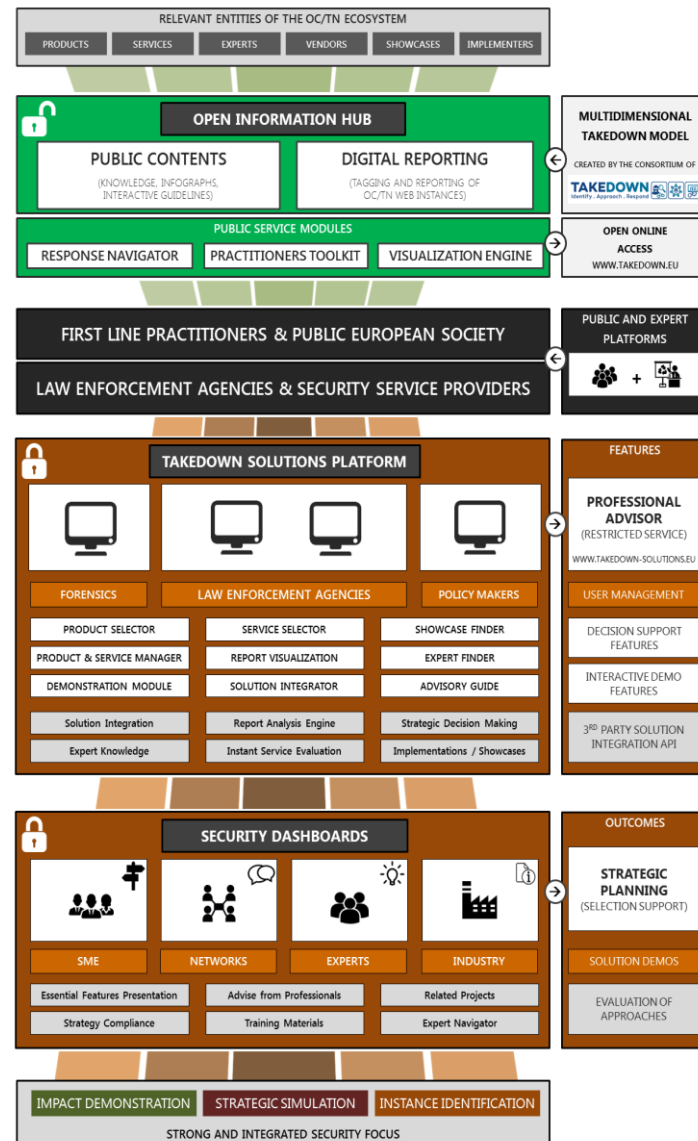
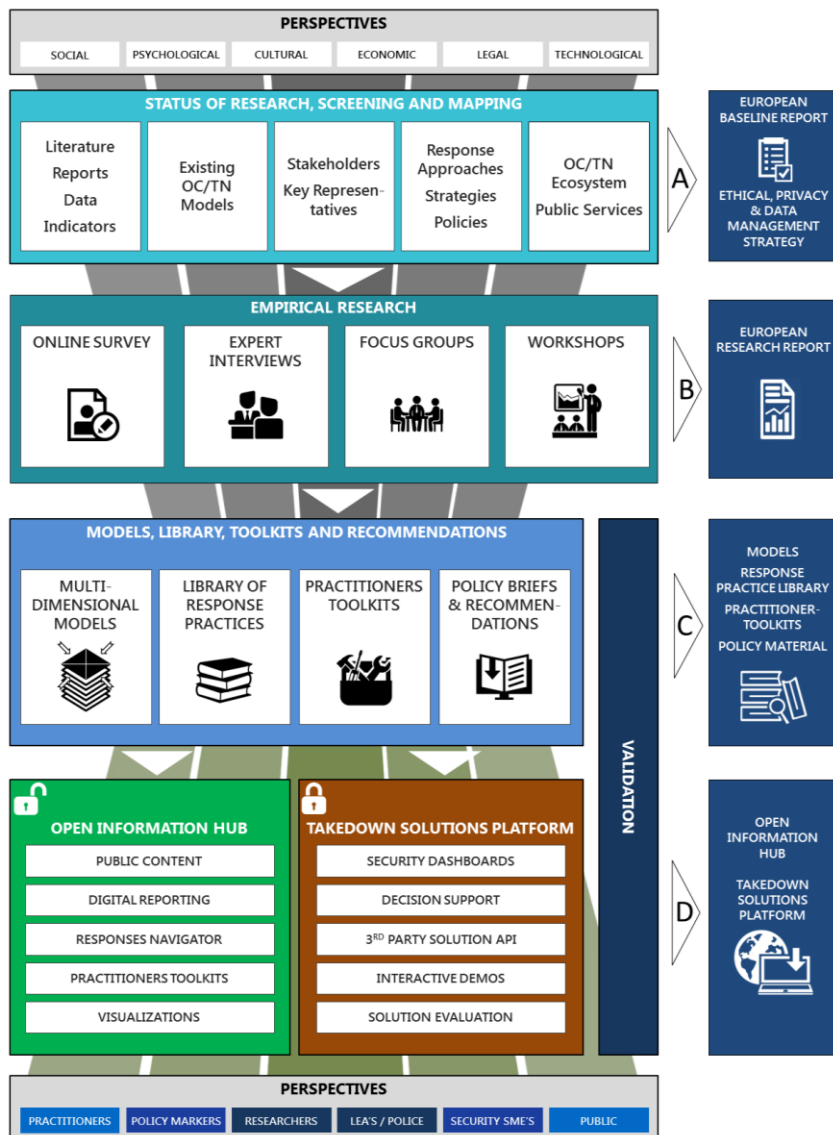
<= **Synthesis**





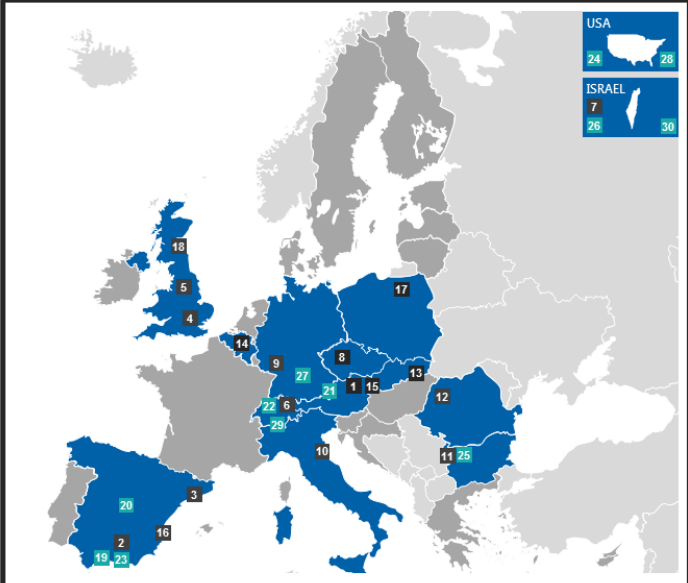














<= **Development/Programming**

<= **Development/Programming**

<= **Networking and Communication**

Project and Platform Concept



<p>1</p> <p>SYNYO GmbH Research & Development Department</p> <p>Vienna AUSTRIA</p> 	<p>2</p> <p>Fundacion Euroarabe de Altos Estudios Projects and Research</p> <p>Granada SPAIN</p> 	<p>3</p> <p>Universitat Autònoma de Barcelona Institute of Law and Technology</p> <p>Barcelona SPAIN</p> 	<p>4</p> <p>Middlesex University Higher Education Corporation Department of Criminology and Sociology</p> <p>London UNITED KINGDOM</p> 
		<p>5</p> <p>University of Leeds Centre for Criminal Justice Studies</p> <p>Leeds UNITED KINGDOM</p> 	<p>6</p> <p>Eidgenössische Technische Hochschule Zuerich Center for Security Studies</p> <p>Zurich SWITZERLAND</p> 
		<p>7</p> <p>Technion Israel Institute of Technology Behavioral Science</p> <p>Haifa ISRAEL</p> 	<p>8</p> <p>Ceske Vysoké Učení Technické v Praze Dept. Of Security Technologies and Engineering</p> <p>Praha CZECH REPUBLIC</p> 
		<p>9</p> <p>Technische Universität Darmstadt Telecooperation Lab</p> <p>Darmstadt GERMANY</p> 	<p>10</p> <p>Agenfor Italia International Projects</p> <p>Rimini ITALY</p> 
<p>11</p> <p>Center for the Study of Democracy Law Program</p> <p>Sofia BULGARIA</p> 	<p>12</p> <p>Peace Action Training and Research Institute of Romania Department of Peace Operations</p> <p>Cluj-Napoca ROMANIA</p> 	<p>13</p> <p>Vysoká škola Bezpečnostného Manažerstva v Kosiciach Nezisková Organizácia Security management</p> <p>Košice SLOVAKIA</p> 	<p>14</p> <p>Leuven Security Excellence Consortium vzw Leaders In Security</p> <p>Heverlee - Leuven BELGIUM</p> 
<p>15</p> <p>Agentur für Europäische Integration und wirtschaftliche Entwicklung</p> <p>Vienna AUSTRIA</p> 	<p>16</p> <p>Ayuntamiento de Valencia European Projects Department</p> <p>Valencia SPAIN</p> 	<p>17</p> <p>Wyższa Szkoła Policji w Szczytnie Institute of Social Sciences</p> <p>Szczytno POLAND</p> 	<p>18</p> <p>Cloud Security Alliance Europe</p> <p>Edinburgh UNITED KINGDOM</p> 

What do the LEAs and other players (such as first-line-practitioners) identify as major challenges and requirements?

⇒ **Aims of the empirical research**

- For getting a better understanding out from the field
- For highlighting the challenges of first-line-practitioners
- For revealing the requirements of the LEAs
- For developing the policy recommendations

=> First insights from the initial analysis with a focus on organized (cyber)crime

=> PUBLIC REPORT will be released end of December 2017
(download on www.takedownproject.eu)

The TAKEDOWN **online survey** gathered data on the practices and views of first-line practitioners and professionals, who are addressing the causes or effects, associated with terrorism and/or **organised (cyber)crime**.

=> Timeline and Scope

The online survey was open from **May 24, 2017 to September 16, 2017** and the analysis includes **519 respondents**.

=> Respondents Profile

- More than **65%** of the respondents are **male**
- The majority is between **30 to 40 years old**
- The survey covers a total of **23 countries, 15 different professions** that fall into the category of first-line-practitioners and **12 different areas of work** within these professions
- **26%** of the respondents were national Law Enforcement Agents/Police Officers

- **CHALLENGES**

- Related to **Organized (Cyber)Crime**, the respondents mentioned that especially *'human trafficking'*, *'drug production / trafficking'* and *'cybercrime'* require more attention, effective prevention and response strategies

- **DRIVERS**

- *'Being raised in a criminal environment'* has the strongest influence on increasing organised (cyber)criminal activities

- **RECRUITMENT**

- *'Recruitment by a friend'* is the strongest recruitment pathway for organised (cyber)crime

- **COUNTERMEASURES**

- Regarding actions for decreasing organised crime, *'Creation of special police / law enforcement units for tackling organised crime'* and *'job creation / employment schemes targeting low-income / at risk communities'* would have the strongest effect

- **Chi-Square (χ^2) Test of independence** (test for a statistically significant relationship between two variables):
 - Series of strong **moderate** and **significant correlations** amongst nearly all of the **economic variables** with each other
 - It suggests that **organised (cyber)criminality** is more about **lack of opportunity** and **additional financial burdens both of the individual, but also within their communities and societies**
 - Hence, “**harder tactics**” are **NOT** seen as the most promising actions against organized (cyber)crime – but **social (economic) welfare** and **social and mental support** had significant associations

- **Germany (Darmstadt) – July the 6th 2017:** Security Solutions against Organized Crime and Terrorist Networks.
- **Italy (Reggio Calabria) – August the 29th 2017:** Towards Security Solutions against Organized Cyber-Crime and Terrorist Networks.
- **Spain (Barcelona) – September the 18th 2017:** Ethical and Legal Issues in Security: Ensuring Data Protection.
- **Belgium (Brussels) – November the 16th 2017:** Darknet, Deepweb and other Cybercrime enabling Organized Crime and Terrorist Networks.

*=> Total of 31 speakers (excl. Consortium members), incl. representatives from **academia, public authorities, private sector and law enforcement agencies***

Main enabling factors of Cybercrime:

- Dematerialization of Illegal Activities
- Increased International Collaborations
- Online Anonymity

Current challenges:

- Social Network analysis, since the use of social networks has been “abused” in the last years for performing, disseminating and advertising illegal activities
- Exploitation and/or implementation of (semi-)automatic solutions that are able to cope with huge amount of data
- Definition of solutions that comply with EU regulations in order to support the collaboration among the states members
- Darknet: for disrupting the activities on the Darkweb, platforms are taken over by LEA specialists => However, such activities are challenging the legal systems and the LEAs because of: securing evidence, cost of operations, waterbed effect, entrapment etc.

Major needs:

- Need for a strong coordination, communication and alignment of national and international laws that are regulating the field of cyber-security
- Need for tools and services that facilitates the coordination and the communication process between nation states and LEAs in order to make investigations easier and improve convictions of transnational cybercrime

⇒ **Coherent with the outcomes of the expert interviews (112 interviews between late 2016 and June 2017)**

- **Additional needs mentioned by experts:**
 - Need for funding and training of law enforcement officers dealing with organized (cyber)crime
 - Addressing the lack of political will to fight organized (cyber)crime if there are links between criminal groups and the political establishment

How can we get to a better understanding of organized (cyber)crime, radicalisation and terrorist networks BEFORE we develop technological solutions?

=> approaching the topic through the analytical TAKEDOWN Model

Aims of the model:

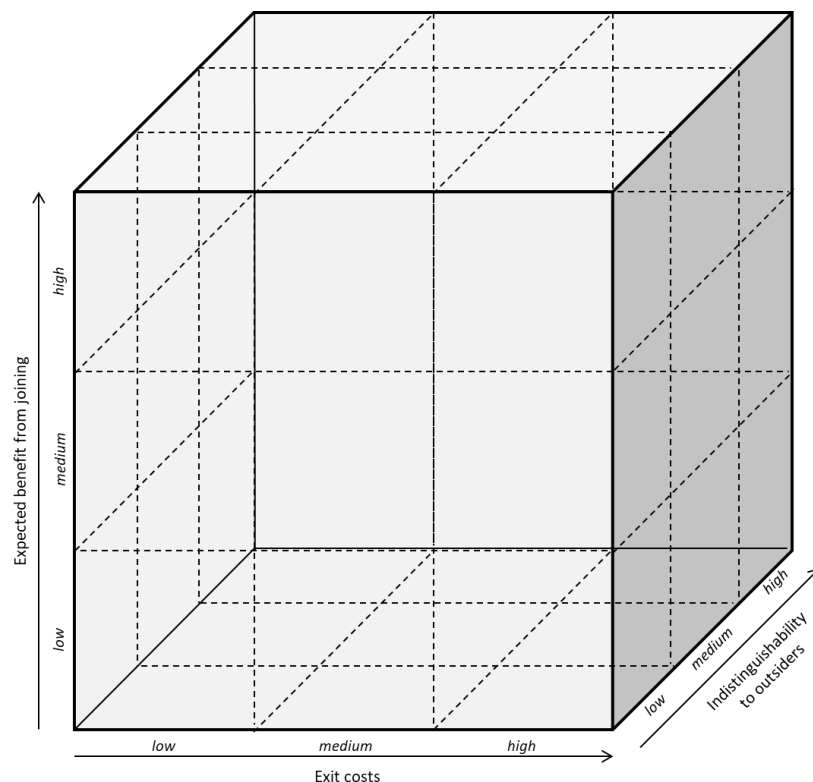
- Intends to provide a holistic understanding of the phenomenon – including trajectories, pathways, dynamics, individual factors and structural conditions
- Informs the practitioner tools (logic of cases, dynamics, implications of counter-measures etc.)
- Basis for the technical developments of the project: Open Information Hub & Solutions Platform (model-based advisory services and decision-making support)
- Advances the body of knowledge/research
- Provides the “intelligence” for solution developers

Requirements for the model development from the literature review and from the empirical research

Model requirement	Level	Effect(s)
Operational under uncertainty	structural	expand user horizon
Dynamic-friendly	structural	avoid reification methodological indistinctiveness
Universally adaptational	structural	multi-stakeholder friendly target-oriented
Self-learning	functional	cross-fertilization ongoing reassessment
Self-reflective	functional	structural sensitiveness social embeddedness
Fundamental rights abiding	normative	legitimacy social acceptance

Dimensions / Axes

- (1) **Exit costs:** captures the cost of exiting the OC/TN environment
- (2) **Benefits from joining:** subjective benefit from joining the OC/TN activity
- (3) **Indistinguishability to outsiders:** captures the ability of the stakeholders (that try to fight the OC/TN activities) to distinguish between members of the organizations/networks and people that are not involved in the illegal activity

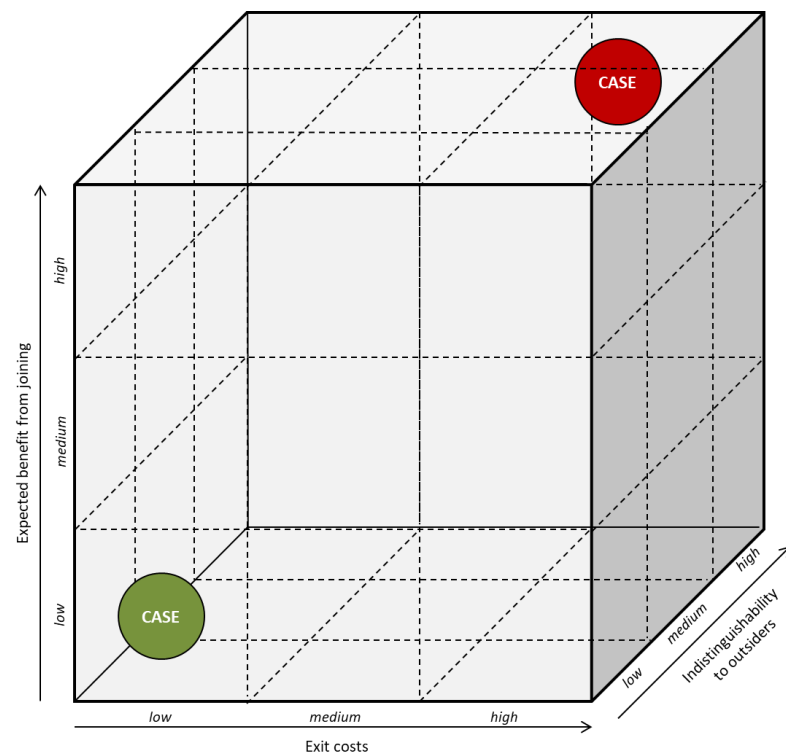


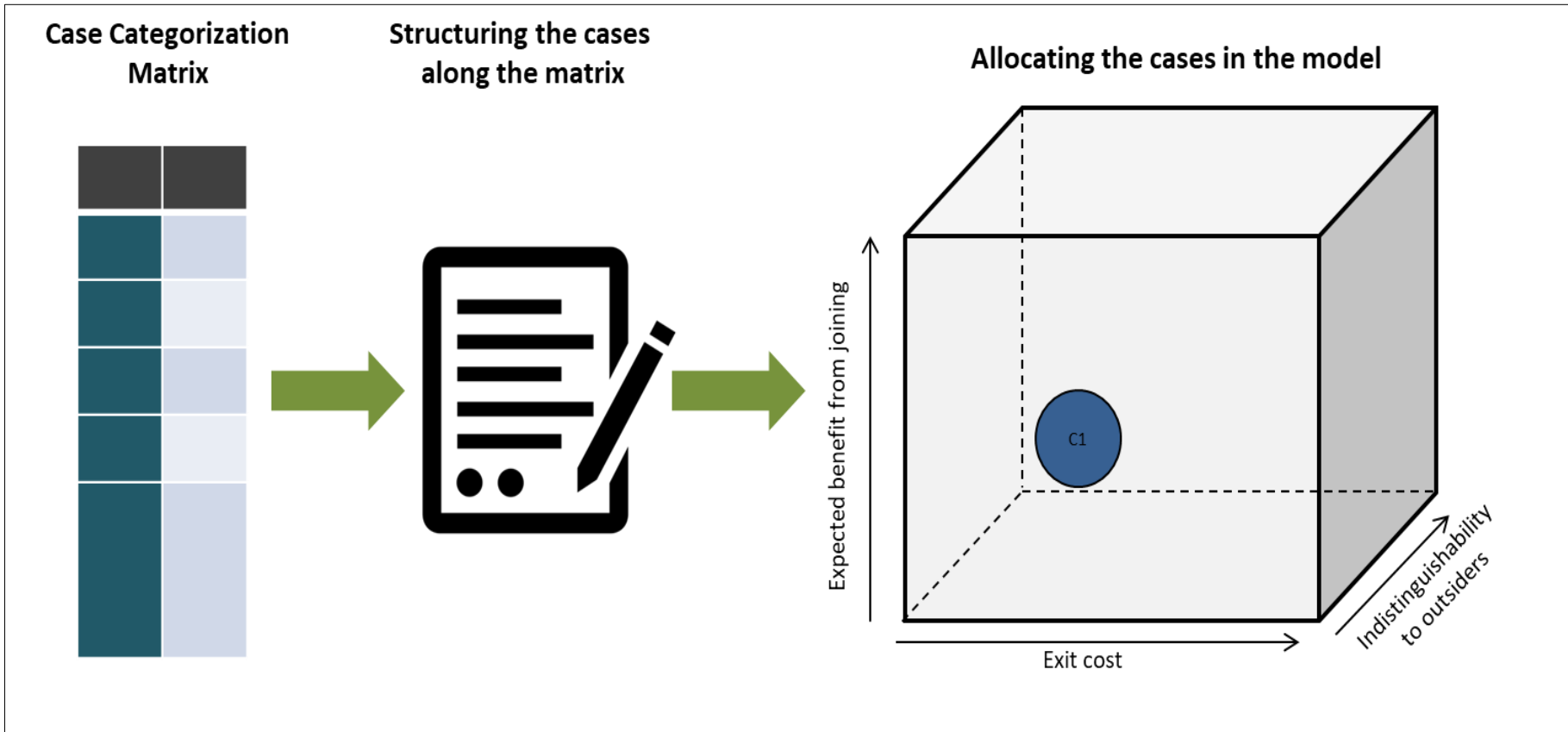
=> Case-driven applications of the model also include **time** as a **fourth dimension**

Cases are located in **different segments** of the cube.

It requires less effort to prevent cases located in the lower, left corner of the cube (**green case**).

Cases in the top, right corner of the cube are much more difficult to address (**red case**).





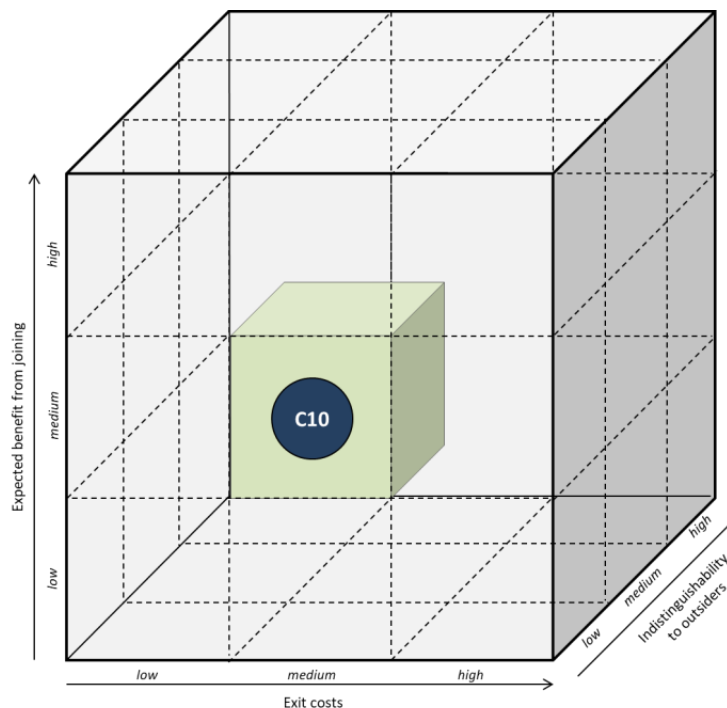
Case categorization matrix

- Areas** (radicalization/terrorism, organized crime and nexus)
- Criminal Methods** (Recruitment, Funding, Training, Execution and Concealment)
- Country and Demographics** (Location of the Case, Age, Sex and Family Background)
- Historical trajectories** (family history)
- Sociological** (Class, Education, Origin, Networks, Societal Embedding)
- Psychological** (Personality , Motivations, Peer Pressure)
- Economic
- Cultural** (Religious Confession, Internalization of Belief Systems and Family values)
- Narratives** (Defense against existential Threat, Identity and Belonging, and Clusters of People)
- Legal** (Citizenship, Residential Status, Crime Record and Record of Domestic Violence)
- Geographical** (Country of Origin and Transnational Ties)
- Technological** (Use of Social Media, Use of anonymous Messenger Services, Use of the Dark Net and general Technological skills)
- Entry Points / Environments** (Schools, Prisons, Neighborhoods, Religious Communities and the Internet)

Area	Sub-Area	Category	Case 1	Case 2	Case 3	Case 4	Case 5
Areas	Radicalization / Terrorism						
Areas	Organized Crime						
Criminal Methods	Recruitment						
Criminal Methods	Funding						
Criminal Methods	Training						
Criminal Methods	Execution and Concealment						
Country and Demographics	Location of the Case						
Country and Demographics	Age						
Country and Demographics	Sex						
Country and Demographics	Family Background						
Historical trajectories	Family history						
Sociological	Class						
Sociological	Education						
Sociological	Origin						
Sociological	Networks						
Sociological	Societal Embedding						
Psychological	Personality						
Psychological	Motivations						
Psychological	Peer Pressure						
Economic							
Cultural	Religious Confession						
Cultural	Internalization of Belief Systems						
Cultural	Family values						
Narratives	Defense against existential Threat						
Narratives	Identity and Belonging						
Narratives	Clusters of People						
Legal	Citizenship						
Legal	Residential Status						
Legal	Crime Record						
Legal	Record of Domestic Violence						
Geographical	Country of Origin						
Geographical	Transnational Ties						
Technological	Use of Social Media						
Technological	Use of anonymous Messenger Services						
Technological	Use of the Dark Net						
Technological	General Technological skills						
Entry Points / Environments	Schools						
Entry Points / Environments	Prisons						
Entry Points / Environments	Neighborhoods						
Entry Points / Environments	Religious Communities						
Entry Points / Environments	The Internet						

CASE 10

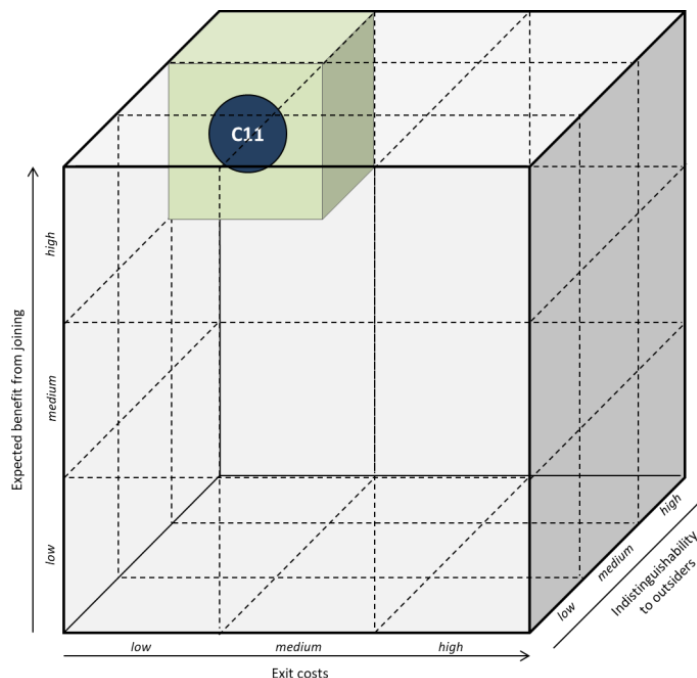
A Swiss banker and his cousin arrested for money laundering



MODEL DIMENSION	HYPOTHESIZED LOCATION & JUSTIFICATION
<i>Expected benefits from joining</i>	medium (the main motivation were comparatively low financial benefits)
<i>Exit Costs</i>	medium (one could assume that the client had enough information on the banker and the cousin, and that the client has the right contacts to really threaten them)
<i>Indistinguishability to outsiders</i>	low (the banker and his cousin were already caught in the execution of their second transport due to border control)

CASE 11

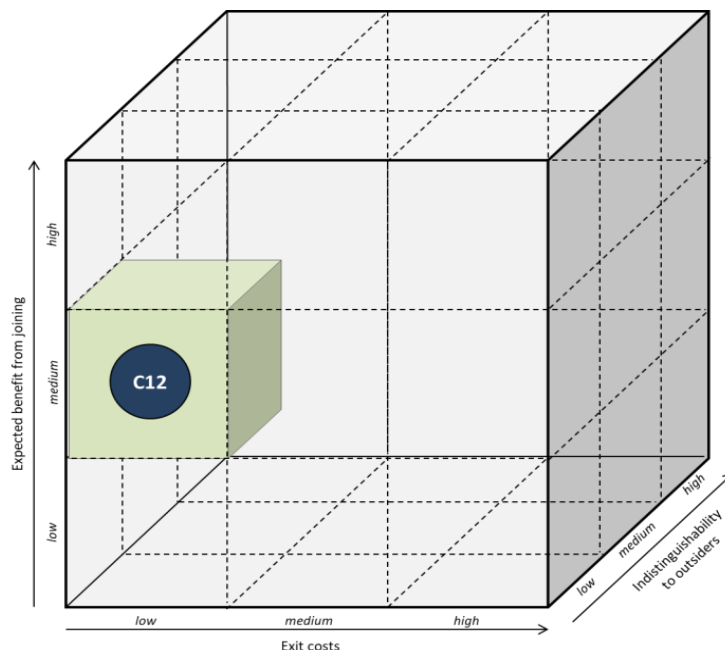
International group of hackers that conducted large scale cybercrime (phishing and online fraud)



MODEL DIMENSION	HYPOTHESIZED LOCATION & JUSTIFICATION
<i>Expected benefits from joining</i>	high (the main motivation for the perpetrators seemed to be financial benefits)
<i>Exit Costs</i>	low (when the case would have remained uncovered, he might have had the chance to disappear; he was also freed from the charges made in Switzerland)
<i>Indistinguishability to outsiders</i>	high (the group operated mainly in cyberspace, was based in Thailand and consisted of individuals of different nationalities; they also often used middlemen when obtaining cash-outs)

CASE 12

Young woman of Moroccan decent and legal resident in Spain, who was radicalised through social media and planned to travel to Syria

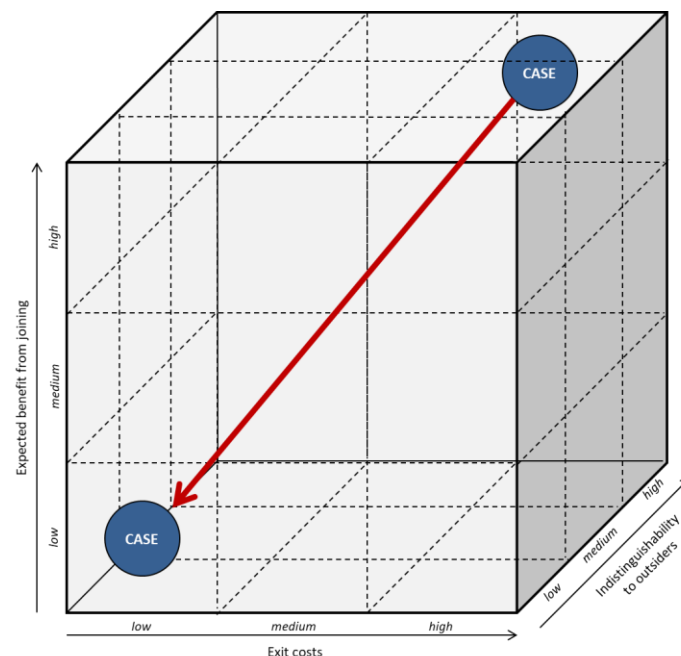


MODEL DIMENSION	HYPOTHESIZED LOCATION & JUSTIFICATION
<i>Expected benefits from joining</i>	medium (as they are mainly related with identity and belonging and is not related to any financial or other benefits)
<i>Exit Costs</i>	low (as the individual actually didn't join yet the IS but was mainly in contact through online networks and – if ever – through physical middlemen)
<i>Indistinguishability to outsiders</i>	low (the activities of the case where mainly online in social media and although by the end she was using fake names etc. she actually started by using her real name)

Previous research shows the values of several interventions that achieve this goal. The most important interventions involve the **expected benefit dimension**. For example, providing the population good education and attractive, legal career options, is known to reduce the tendency to join OC/TN.

Moving a OC/TN case along the **exit cost dimension** is more difficult. Exit costs are particularly large when the OC/TN involvement develops within a close-knit network, peer group or family ties. One example for a successful response that reduces exit costs is the implementation of principal witness programs using strong incentives such as monetary incentives, reduced punishment, and a secure future.

Decreasing **indistinguishability** is often a technological task or can also be done indirectly. For example, principal witness programs, when successful, can provide authorities with detailed information regarding the TN/OC case, reducing indistinguishability of its members.



Tracing the pathways of cases (terrorism case => Perpetrator of the 2016 Normandy Church attack)

- **From L1 to L2:** Coming from a non-religious background, Case 1 had a rather rapid radicalization process; the closer surrounding didn't really notice it; but when the individual was arrested for trying to travel to Syria, the case became recorded, but he offered to go on parole

=> **expected benefits from joining remaining medium; decreasing exit cost; decreasing indistinguishability to outsiders**

- **From L2 to L3:** Case 1 tried to enter Syria again, but was caught and held in preventive custody for several months; he was approved for house arrest with an electronic tag and to go under 'supervision and support' of his close family and local social welfare institutions; everything was put in place for his de-radicalization and re-integration into society

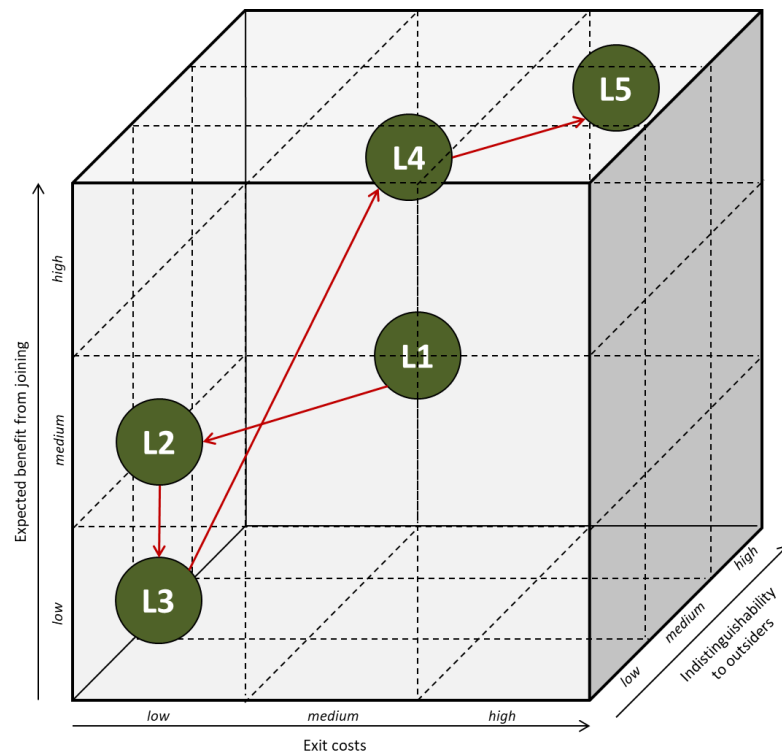
=> **decreasing expected benefits from joining; exit costs remaining low; indistinguishability to outsiders remaining low**

- **From L3 to L4:** The individual was sure that joining the IS or carrying out an attack would help him to overcome his depressions and his need for admiration; over several months he was more and more drawn into this idea

=> **significantly increasing expected benefits from joining; increasing exit costs; increasing indistinguishability to outsiders**

- **From L4 to L5:** Case 1 was able to use of a crypto-messenger service for fining a collaborator and for planning the attack; for unknown reasons the electronic tag was deactivated on the day of the attack; finally the individual carried out the attack

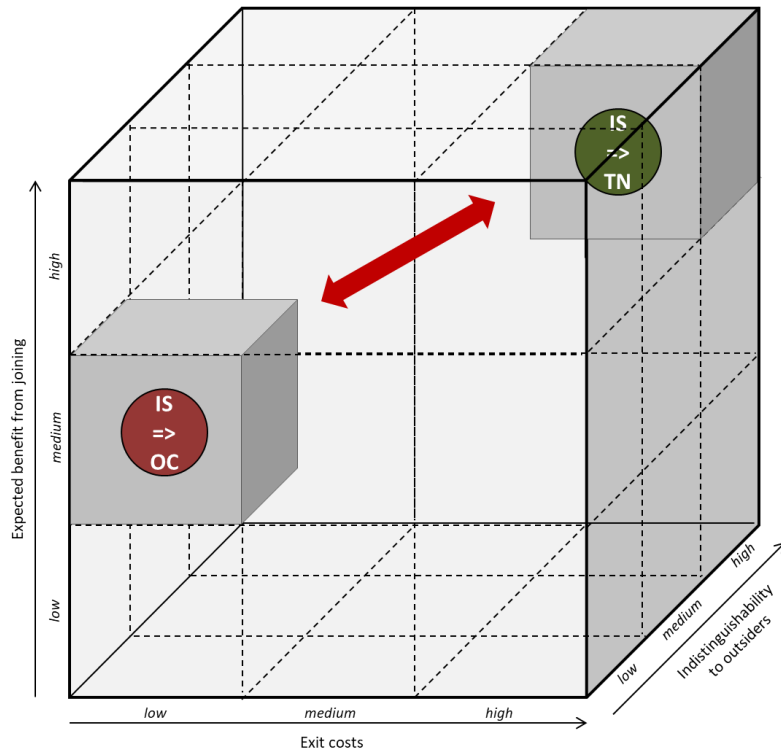
=> **expected benefits from joining remaining high; increasing exist costs; increasing indistinguishability to outsiders**



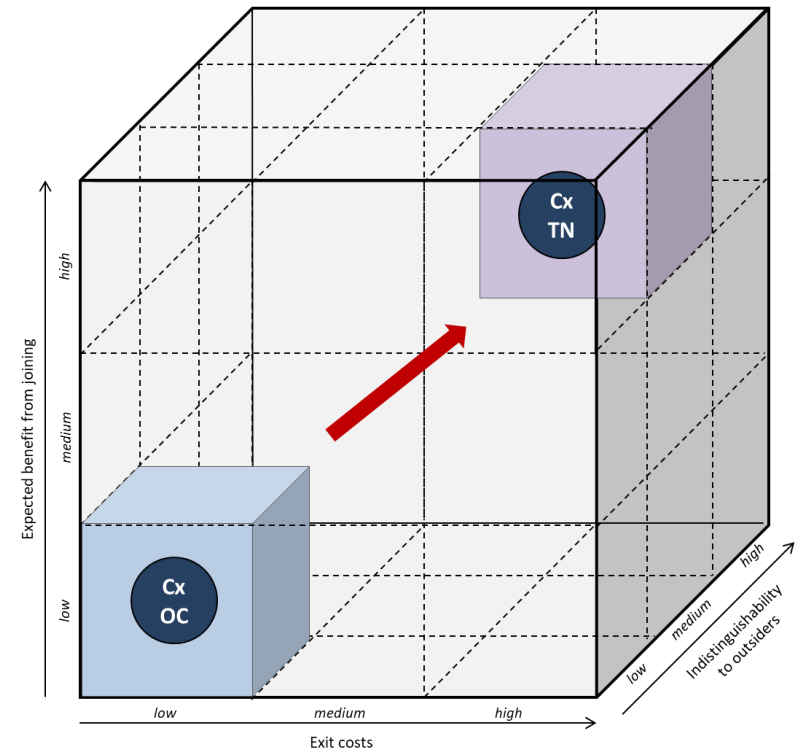
The more information on a case is available, the more precise the different locations and the pathways can be reproduced!

Integrating the OC/TN-NEXUS into the model

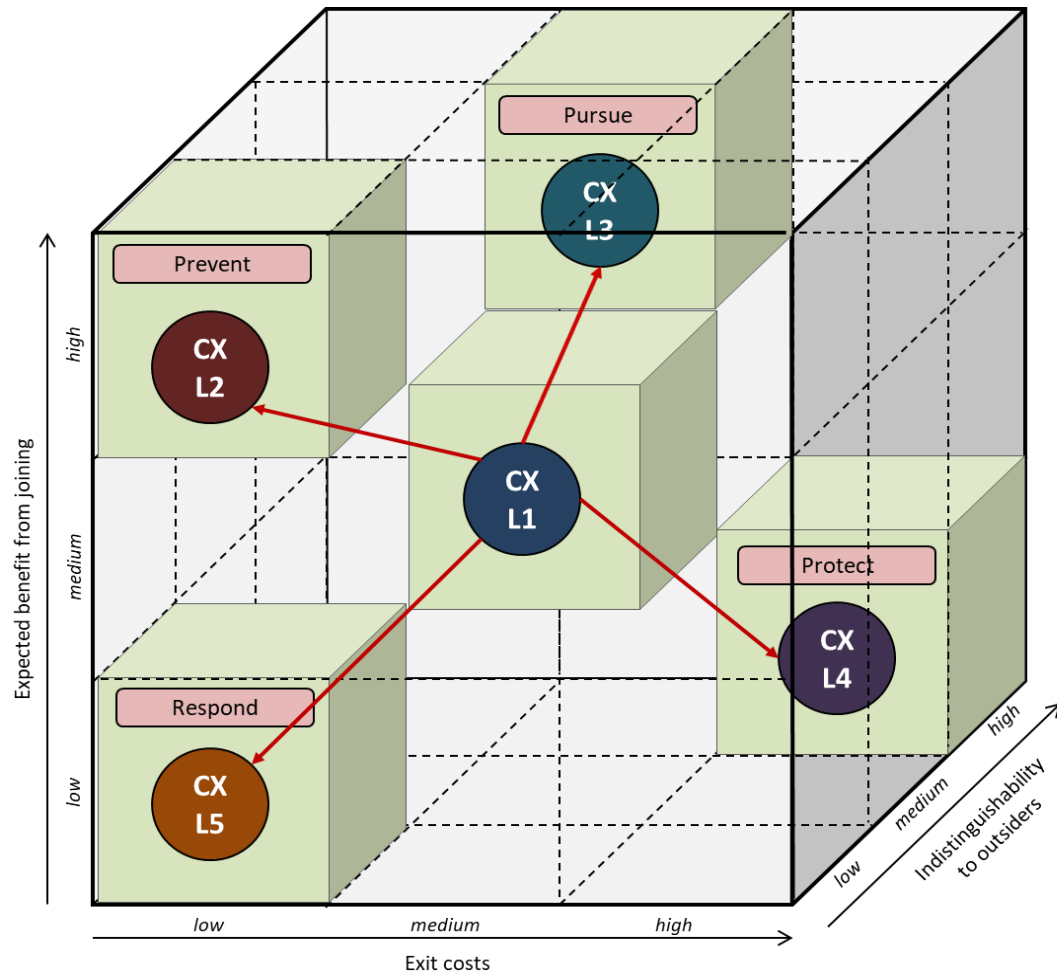
Activities of a case or organisation that is active in both fields (OC/TN)



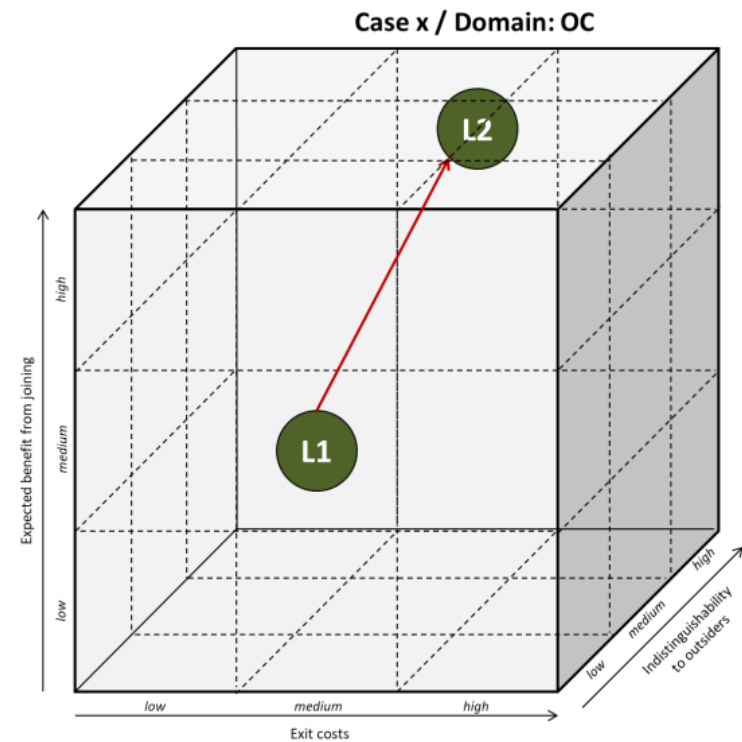
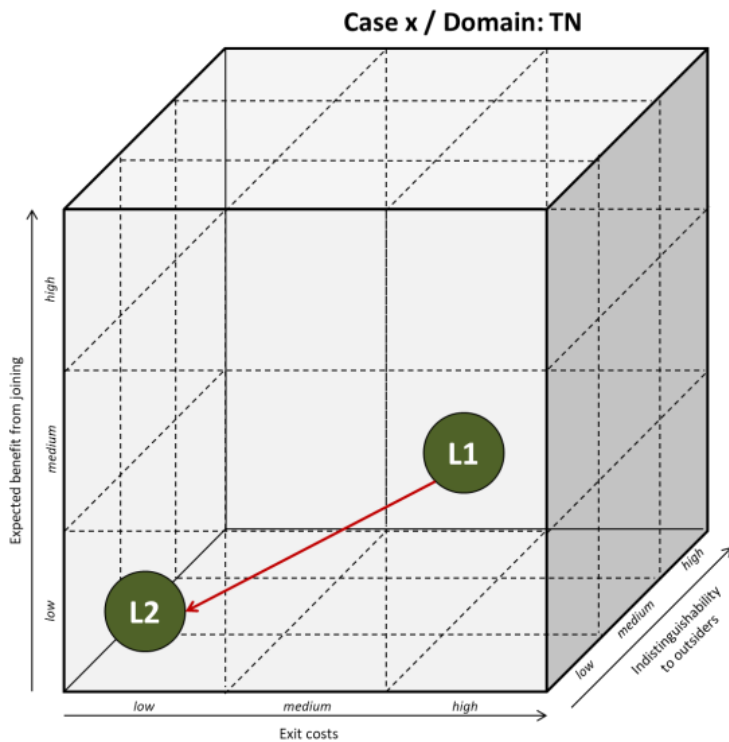
Movement from a case from OC to TN



Understanding the (un)intended consequences of countermeasures



Impact of the counter-measures in case of Nexus



- **Current activities:**
 - Finalizing the empirical research (public report, Dec. 2017)
 - Conceptualizing the TAKEDOWN platforms
- **What lies ahead?**
 - Development of the open information hub and the solutions platform and integrate advisory tools/decision-making support
 - Transfer the models into actual platform application modules and tools for example for Practitioner Decision Support
 - Implement a profound and extensive testing and validation phase
 - Promote the platforms and attract companies/developers/projects to present their demonstrators and solutions on the platform

TAKEDOWN

Identify . Prevent . Respond



www.takedownproject.eu

Dr. Florian Huber

SYNYO GmbH, Vienna (AT)

florian.huber@synyo.com