EUROPEAN UNION AGENCY FOR CYBERSECURITY

European Union
EXTERNAL ACTION

FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI) AND CYBERSECURITY - THREAT LANDSCAPE

DECEMBER 2022

CONTACT

AUTHORS

LEGAL NOTICE

COPYRIGHT NOTICE

FIMI

- **For cybersecurity**
- **For FIMI**

- **Role of cybersecurity in FIMI/disinformation**

- **Importance of structured and seamless incident reporting between the cybersecurity and FIMI/disinformation community**

- **Mutual exchanges between the cybersecurity and the FIMI/disinformation community could benefit the fight against FIMI/disinformation.**

1.1 CONTEXT

Misinformation

disinformation

Foreign Information Manipulation and Interference

1.2 SCOPE

- **Describe FIMI/disinformation, creation and dissemination behaviours as a way to expose the activities the EU aims to prevent, deter and respond to**
- **Show the role of (or lack of thereof) in the production of FIMI/ disinformation, by identifying the underlying cybersecurity elements**

- **For cybersecurity**
- **For FIMI**

IMPORTANT

1.3 TARGET AUDIENCE

1.4 STRUCTURE

- **Section 2**
- **Section 3**
- **Section 4**

2.1 OVERVIEW

Table 1

Categories	Description
Sectors (Primary and secondary)	
Severity	
Duration	
Impact	
Threat actors	
Motivation	
MITRE ATTA&CK	
DISARM	

2.2 SECTORS AND VICTIMS AND IMPACT

-
-

Table 2:

Categories	Primary	Secondary

-
-
-
-
-
-

Table 3:

Victims	Definition

2.3 SEVERITY AND DURATION

-
-

duration

severity **impact**

able 4:

Duration	**Definition**

w947.28 0 Td[6-13.3 (ow)]TJ0 Tc 0 Tw 0.613 0 Td) (y0.7 ( )]TJEMC ET/Artifact #MCI 12

2.4 THREAT ACTORS AND MOTIVATION

Table 6:

Threat Actor	Definition

-
-
-
-
-
-

2.5 DISARM FRAMEWORK AND MITRE ATT&CK

IMPORTANT **As reported above, relevant statistics and findings are presented; however, it needs to be highlighted that the findings are dependent on the limited set of specific incidents analysed and that this report is designed to give a first indication as food-for-thought. Future, much richer datasets and further research will bring better insight**

3.1 DATA COLLECTION AND CLEANING

FIMI/disinformation events

events **information/cyber incidents** **information operation**[26] **information/cyber incidents** **information** **information/cyber incidents**

events **information/cyber incidents** **information operations**

3.2 APPLICATION OF THE PROPOSED APPROACH – DATA ANALISYS

3.2.1 Sectors, victims and impact

Figure 1:

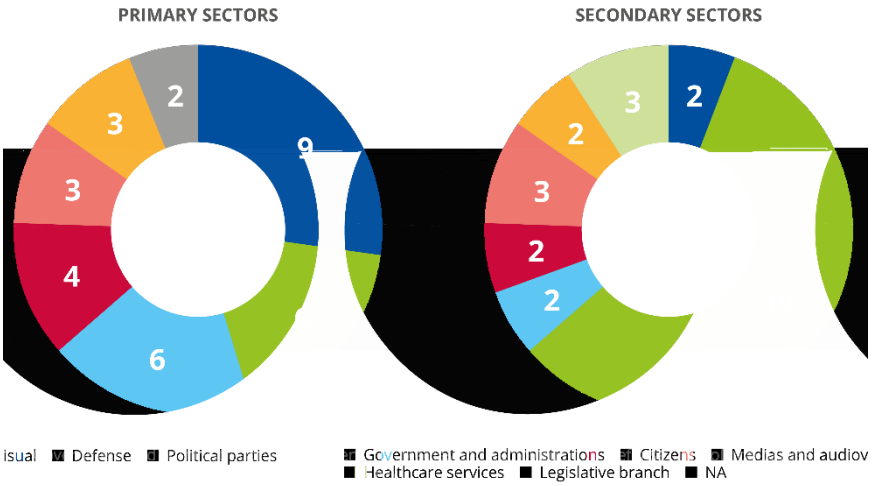


Figure 2:

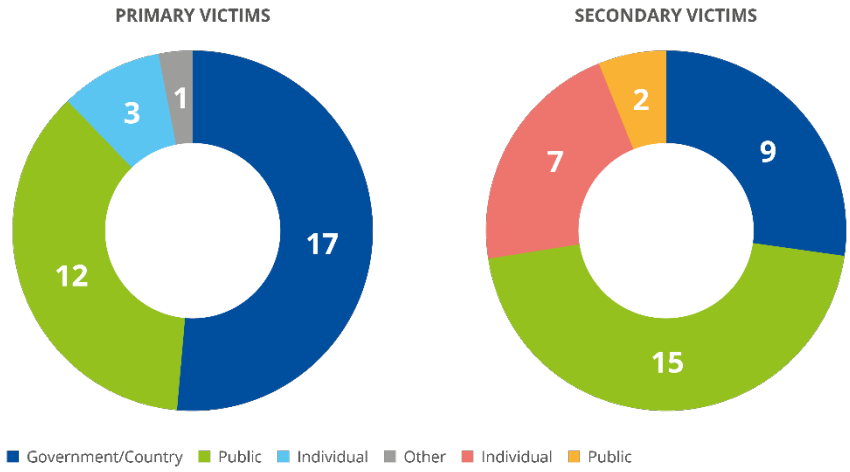
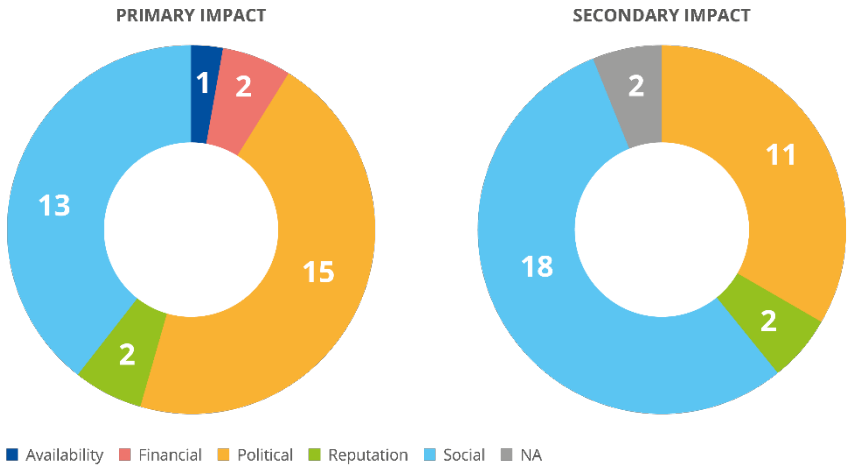


Figure 3:



3.2.2 Severity and duration

Figure 4:

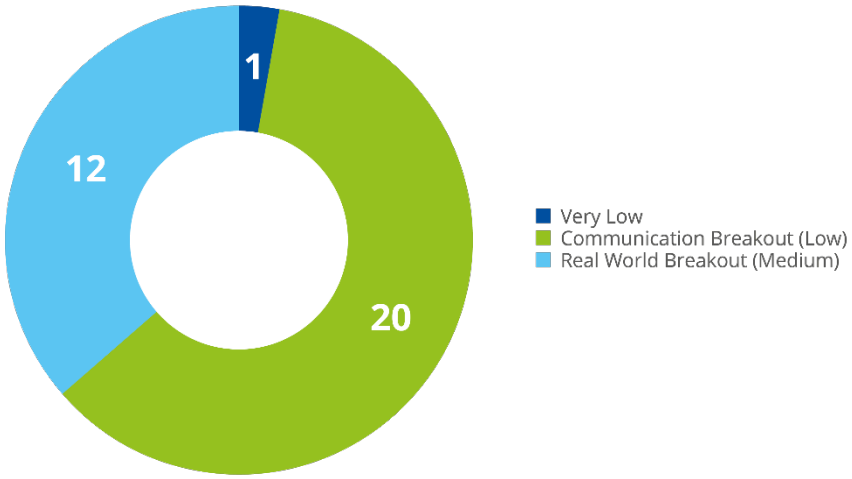
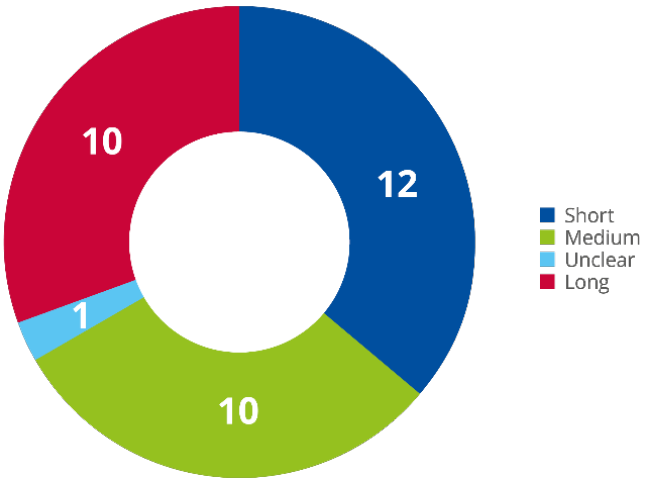


Figure 5:



3.2.3 Threat actors and motivation

Figure 6:

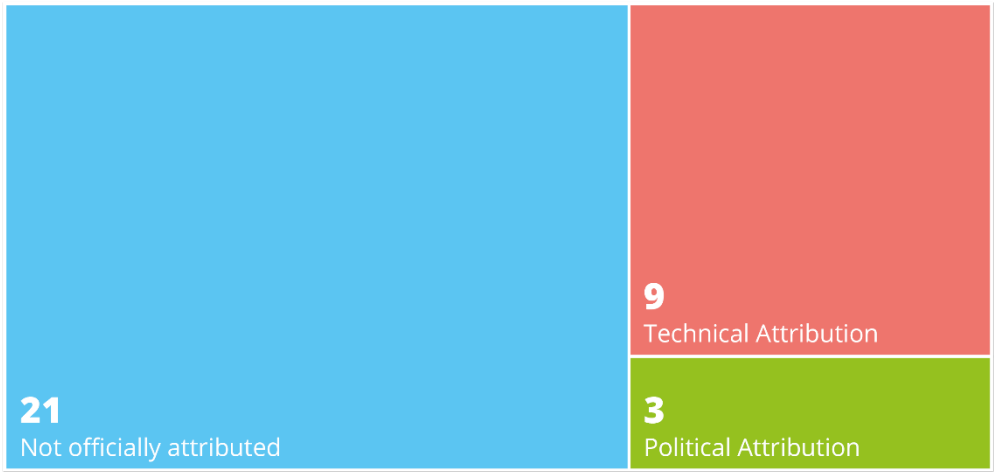
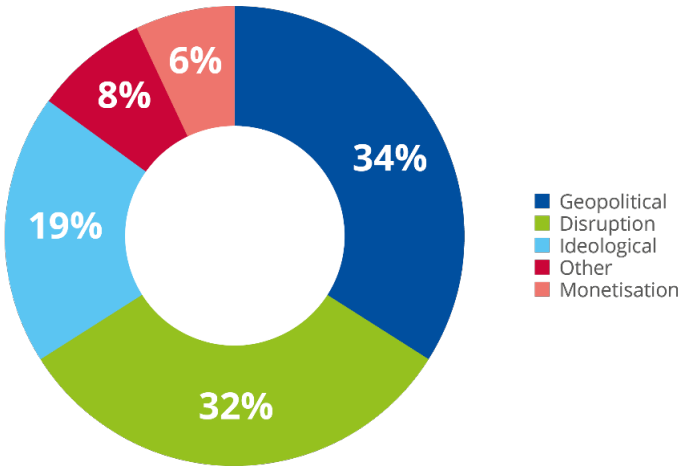


Figure 7:



3.2.4 DISARM framework and MITRE ATT&CK

3.2.4.1 DISARM Framework perspective

Figure 8:

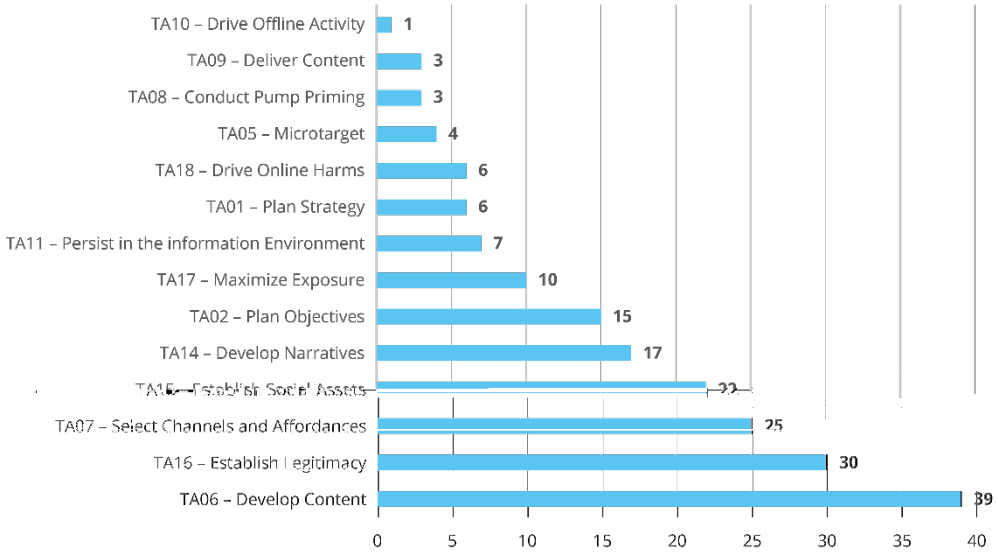


Table 7:

DISARM Tactic	Definition
TA06 - Develop Content	
TA16 - Establish Legitimacy	
TA 07- Select Channels and Affordances	
TA15 - Establish Social Assets	
TA14 - Develop Narratives	
TA02 - Plan Objectives	
TA17- Maximize Exposure	

3.2.4.2 MITRE ATT&CK Framework perspective

Figure 9:

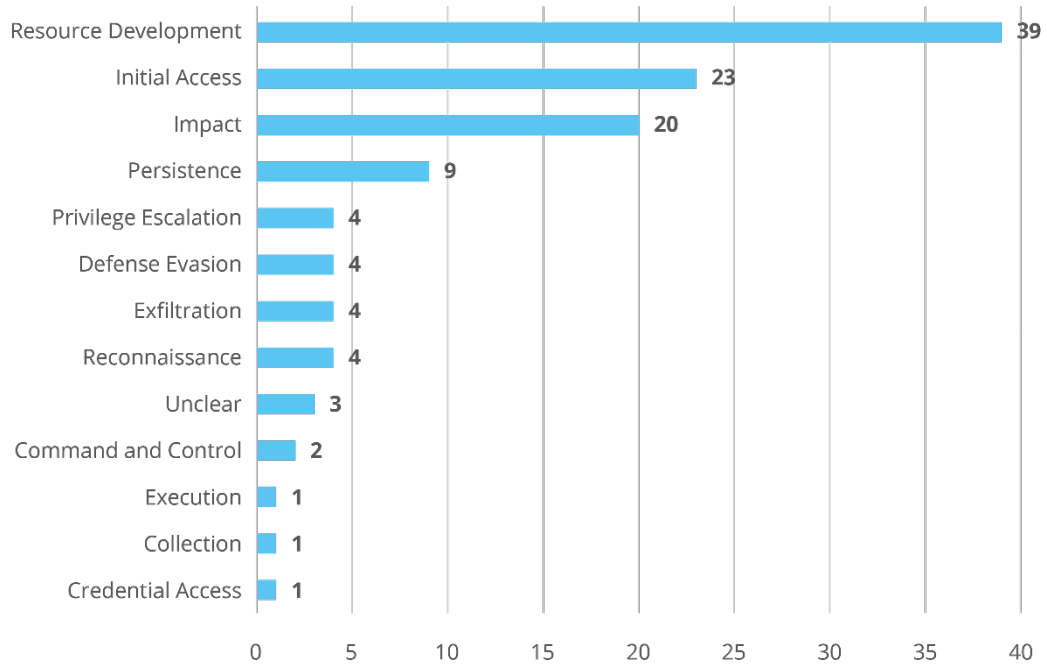


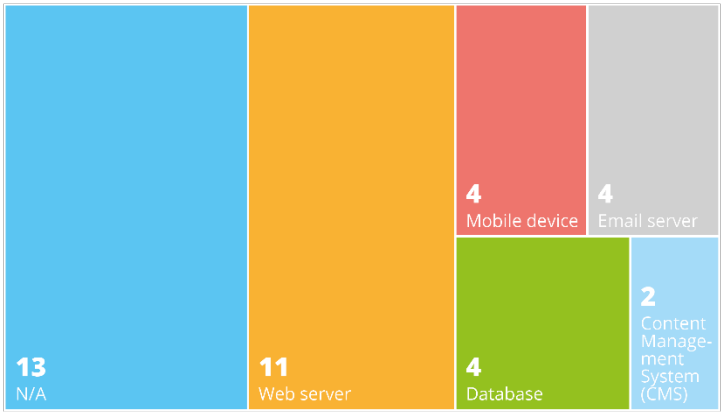
Table 8:

MITRE ATT&CK Tactic	Definition
Resource Development	
Initial Access	
Impact	

3.2.4.3 DISARM and MITRE ATT&CK: Joint perspective and the role of cybersecurity

Figure 10:

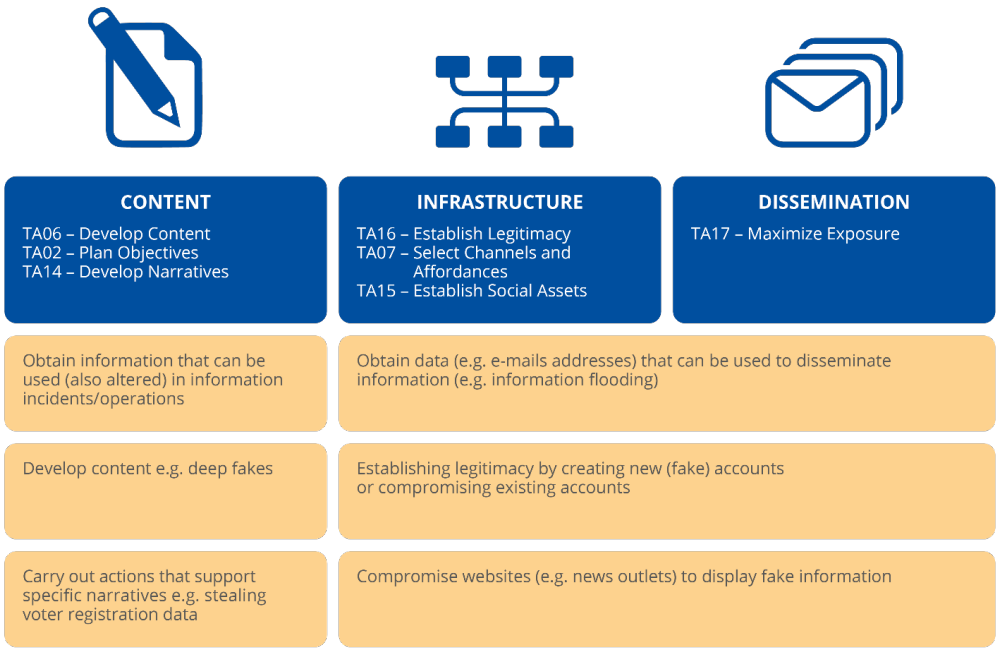
Table 9:



* Each event might be associated to more than one asset

3.2.4.4 The role of cybersecurity

Figure 11:



4.1 TECHNICAL

4.1.1 On the analytical framework

-
-

-

- **Distinction between information/cyber *incidents* and *operations*.**

- **Difficulties in establishing the duration of events**

- **DISARM vs MITRE: the importance of focusing on DISARM tactics to analyse the cybersecurity component of information events.**

- **The primary target (in terms of victims, sectors and impact) is often not the real/main one**

- **FIMI/disinformation events do not necessarily target critical sectors.**

4.1.2 On the role of cybersecurity

- **The role of cybersecurity seems to be particularly important in establishing attribution**

- **The role of cyber-attacks at the initial stages of some FIMI/disinformation events, strengthens the idea that, on the ground, the detection of specific MITRE ATT&CK TTP(s) could act as an indicator of a FIMI/disinformation event.**

- **One of the most relevant limitation in the analysis of the considered FIMI/disinformation events has been the quality of the data. Open-source data about FIMI/disinformation events might not contain sufficient information about its cybersecurity aspects., FIMI/Disinformation reporting should consider this aspect more systematically.**

- **Another limitation has been the comparability of different events, hence reporting needs to be made as coherent as possible.**

- **The role of cyber-attacks at initial stages leads also to another recommendation: awareness raising is important to limit the development or acquisition of content and the compromise of infrastructure that facilitate dissemination.**

4.2 STRATEGIC

- **Foster mutual exchanges between the cybersecurity and FIMI/disinformation community**

- **Improve the availability and quality of FIMI/disinformation incident information**

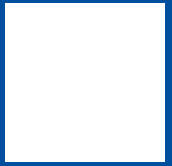
- **Adopt and adapt standard information formats for sharing FIMI/disinformation intelligence**

4.3 POLICY

- **Facilitation of cooperation between those groups should be a priority, especially in crises and surrounding important events such as the upcoming 2024 European Elections**
- **These expert teams jointly should build capacity and capability of Member States and international partners, not only to raise awareness of the importance to bridge the silos, but also to support them to increase their own capabilities**

DISARM Tactic	Top 3 MITRE tactics	
TA06 - Develop Content		
TA16 - Establish Legitimacy		
TA 07- Select Channels and Affordances		
TA15 - Establish Social Assets		
TA02 - Plan Objectives		
TA14 - Develop Narratives		
TA17- Maximize Exposure		

ENISA
Europ



enisa.europa.eu