enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

European Union
EXTERNAL ACTION

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

DECEMBER 2022

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use etlteam@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

ENISA: Erika Magonara, Apostolos Malatras

EEAS: EEAS Strategic Communication Task Forces and Information Analysis Division (SG.STRAT.2)

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-606-4, DOI: 10.2824/7501

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The EU Agency for Cybersecurity (ENISA) and the European External Action Service (EEAS) have joined forces to study and analyse the threat landscape concerning Foreign Information Manipulation and Interference (FIMI) and disinformation. A dedicated analytical framework is put forward, consistent with the ENISA Threat Landscape (ETL) methodology, with the aim of analysing both FIMI and cybersecurity aspects of disinformation.

The concept of Foreign Information Manipulation and Interference (FIMI) has been proposed by the EEAS, as a response to the call of the European Democracy Action Plan[1] for a further refinement of the definitions around disinformation. Although disinformation is a prominent part of FIMI, FIMI puts emphasis on manipulative behaviour, as opposed to the truthfulness of the content being delivered. Several strategic documents, such as the Strategic Compass for Security and Defence and the July 2022 Council Conclusions on FIMI, refer to the importance of countering FIMI as well as hybrid and cyber threats.

FIMI

Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.

Accordingly, in light of broader hybrid threats that cross different domains, one of the main motivations behind this report is to identify ways to bring the cybersecurity and counter-FIMI communities closer together. The ambition is to provide an input to the on-going and ever-pressing discussion on the nature and dynamics of information manipulation and interference, including disinformation, and on how to collectively respond to this phenomenon.

The report proposes and tests an analytical approach describing FIMI and manipulation of information, as well as the underlying cybersecurity elements, by combing practices from both domains:

- **For cybersecurity**: The open methodological framework[2] used by ENISA's annual report on the state of the cybersecurity threat landscape, the ENISA Threat Landscape Reports[3]
- **For FIMI**: The open-source DISARM framework used to capture FIMI/disinformation

By testing the framework on a limited set of events, the report serves as a proof of concept for the interoperability of the frameworks. In addition, it puts forward some preliminary conclusions on the relationship between cybersecurity and FIMI/disinformation:

- **Role of cybersecurity in FIMI/disinformation**. Cybersecurity analysis seems to be particularly important in establishing attribution: among the events analysed, those that had been attributed relied on a cybersecurity analysis. In addition, cyber-attacks seem to be more prominent at the initial stages of FIMI/disinformation events. This means firstly that specific cyber-attack techniques could act as an indicator of a FIMI/disinformation event and, secondly, that awareness raising is important to limit the development or acquisition of content and the compromise of infrastructure that facilitate dissemination.
- **Importance of structured and seamless incident reporting between the cybersecurity and FIMI/disinformation community**. Consistency of data and data quality are the main limitation to cross-domain analyses. For example, open-source data about FIMI/disinformation events often cover entire operations encompassing several incidents, whereas a "pure" cybersecurity perspective would tend to focus on

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0790&from=EN
[2] See https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology
[3] See https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

single incidents. Also, data about FIMI/disinformation events might not contain sufficient information about its cybersecurity aspects. In both cases, improved incident reporting practices could help.

- **Mutual exchanges between the cybersecurity and the FIMI/disinformation community could benefit the fight against FIMI/disinformation.** Since incident handling and response has been at the core of the cybersecurity community for many years, established cybersecurity practices can help the counter FIMI/disinformation community speeding up analytical maturity. For example, the FIMI community can adopt and adapt standard information formats widely used in the cybersecurity realm, to move beyond information sharing by written reports. Conversely, the FIMI/disinformation community can, in return, inform cybersecurity practitioners on new and emerging motivations, targets and threat vectors.

This report has been validated and supported by the ENISA ad hoc Working Group on Cybersecurity Threat Landscapes (CTL)[4].

[4] https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

1. INTRODUCTION

1.1 CONTEXT

This chapter details the concepts used in the report to describe and define manipulation of information, focusing on the activities the EU aims to address and explaining why the terminology commonly used might not be sufficiently comprehensive and precise.

One of the most important parameters in defining the manipulation of information is the notion of "intent". "**Misinformation**", i.e. the *unintentional* spread of false and/or misleading information, differs from the *intentional* manipulation of the information environment. The importance of this basic distinction is the repertoire of response options that can be used for *unintentiona*l misinformation versus *intentional* information manipulation. Responses like exposing the actors responsible for such activity is adequate if actors engage in intentional, coordinated and systematic manipulation, but not if they are individual citizens who merely believed a false/misleading piece of information. Misinformation falls outside the scope of this report.

Intentional attempts to manipulate the information environment and public discourse by foreign actors is by no means a new phenomenon. However, activity which has previously been described as "propaganda" and more recently as "disinformation" has received a considerable new impetus by technological advancements and the propagation of the internet, in particular social media and private messenger services. With this development, new ways of manipulation have become available to malicious actors. In the last years, the term "**disinformation**", intended as the intentional spread of false and/or misleading information for a specific purpose, has become well-known and broadly used. However, this definition of disinformation captures only part of the problem: the manipulation of the content that is being pushed to distort facts and reality, to foster fear and hatred and to sow division in societies. Other terms have also been developed, such as "computational propaganda", "coordinated inauthentic behaviour" or "information pollution", to name just a few. These either incorporate new aspects in addition to disinformation intended as above or they depict activities that go beyond its focus on content.

The current over-abundance of terms and concepts could hamper effective responses and lead to confusion over which phenomena or aspects thereof are actually being addressed. This is exacerbated by the fact that the stakeholders countering such threats are diverse: from international organisations to governments (national, regional and even local), private industry and civil society. Therefore, it is necessary to go beyond the surface and be more specific in describing the manipulation of the information environment the EU aims to address.

Accordingly, the European Democracy Action Plan[5] called for the further refinement of the definitions, in close cooperation with stakeholders. The European External Action Service (EEAS) has proposed the definition of "**Foreign Information Manipulation and Interference**":

"Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory."

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0790&from=EN
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

The concept of FIMI puts emphasis on manipulative behaviour as the main indicator of an attack instead of content and its truthfulness. From this perspective, the manipulation of the information environment is only one aspect of FIMI, although a prominent one.

The need to further step up the EU's efforts in the area of FIMI has been highlighted in the recent Council Conclusions on FIMI[6] . Also, the Strategic Compass for Security and Defence[7] stresses that FIMI does not only constitute a threat to democracy, but also to our security. Russia's use of information manipulation and interference in the preparation and execution of its war of aggression against Ukraine demonstrates this and shows how such activity constitutes an integral part of modern warfare.

Cybersecurity is an important aspect of this context. Firstly, hybrid threats make use of combinations of cyberattacks and information manipulation to successfully materialise. Therefore, a comprehensive analysis of related phenomena has to encompass the cybersecurity domain. Secondly, a thorough understanding of the tactics, techniques and procedures (TTPs) used by malicious actors is crucial for effective response to threats – this corresponds to the part of the FIMI definition which speaks about a "pattern of behaviour" and "activity [that is] manipulative in character". In the cyber domain working with TTPs has been an established practice for many years and can inform approaches to counter-FIMI.

1.2 SCOPE

The objective of the report is to propose and test an analytical approach describing FIMI and manipulation of information (hereby referred to as "FIMI/disinformation") as well as the underlying cybersecurity elements. The peculiarity of such approach is in the combination of practices from both the counter-FIMI and the cybersecurity communities in order to:

- **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**

To do so, the proposed approach relies on two pillars:

- **For cybersecurity**: The open methodological framework[8] used by ENISA's annual report on the state of the cybersecurity threat landscape, the ENISA Threat Landscape Reports[9]
- **For FIMI**: The open-source DISARM framework used to capture FIMI/disinformation

In light of broader hybrid threats that cross different domains, one of the main motivations behind this approach is to identify ways to bring the cybersecurity and FIMI communities closer together. In this respect, the approach showcases how work on FIMI/disinformation can benefit from approaches from the cyber domain where e.g. working with TTPs has been an established practice for many years.

A considerable part of the approach builds on the idea that a concurrent analysis of relevant events by means of specialised frameworks that adequately describe the characteristics of the respective domains (cybersecurity and FIMI) can yield significant intelligence and amplify joint situational awareness - therefore allowing better identification and protect against FIMI/disinformation.

By testing the proposed approach on a real set of events, the report serves as a proof of concept for the interoperability of the frameworks. In addition, it puts forward some preliminary conclusions on the relationship between cybersecurity and FIMI/disinformation.

IMPORTANT: 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

[6] https://data.consilium.europa.eu/doc/document/ST-11429-2022-INIT/en/pdf
[7] https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en
[8] See https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology
[9] See https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

designed to give a first indication as food-for-thought. Future, much richer datasets and further research will bring better insight.

As stated above, a shared understanding on how to describe the manipulation of the information environment is key for the detection of malicious activities, information sharing and response. Against this context, the proposed approach should not be intended as a final product, but rather as an initial, operational contribution to this common effort. Ultimately, the ambition is to provide an input to the on-going and ever-pressing discussion on the nature and dynamics of information manipulation and interference, including disinformation, and on how to collectively respond to this phenomenon.

1.3 TARGET AUDIENCE

The audience of the report consists of policy-makers, as well as of practitioners and academics from both the counter-FIMI/Disinformation and cybersecurity communities, who could use and/or enhance the proposed approach to describe FIMI/Disinformation incidents and define countermeasures.

1.4 STRUCTURE

The report is structured as follows:

- **Section 2** presents the proposed approach, including a general overview and its categories and definitions
- **Section 3** shows how the proposed approach has been applied and tested on a limited set of events.
- **Section 4** outlines the conclusions and recommendations on different levels: technical, strategic and political

2. PROPOSED APPROACH

As explained above, the two pillars of the proposed approach are, on one hand the framework used by ENISA's annual report on the state of the cybersecurity threat landscape, the ENISA Threat Landscape Reports[10], and, on the other hand, the DISARM. The former has been adapted and complemented with practices from the counter-disinformation community, in particular with respect to the severity and the disinformation tactics.

2.1 OVERVIEW

The table below shows an overview of the proposed approach, which is expanded in the subsequent sections:

Table 1: Overview of the analytical framework[11]

Categories	Description
Sectors (Primary and secondary)	Open Cyber Threat Intelligence (Open CTI) Platform
	EU Directive 2016/1148 (NIS Directive)
Severity	Reach of a FIMI/disinformation event
Duration	Short/Medium/Long
Impact	Domains affected
Threat actors	Technical or political attribution to a state, non-state actor or proxy
Motivation	Reason underlying an information event
MITRE ATTA&CK	MITRE ATT&CK for Enterprise[12]
DISARM	DISARM (DISinformation Analysis & Risk Management) Red framework[13]

2.2 SECTORS AND VICTIMS AND IMPACT

The classification of the sectors and victims has been defined in order to reflect the fact that an event directly affecting one sector/one victim or having a specific direct impact, might be designed to target another sector/another victim and to have another impact. As an illustration, the primary target could be the holder of a social media account that an actor breaches to gain control, but the secondary target (the one that is the intended target of an actor) could be the followers of the account.

[10] See https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends
[11] One of the feedbacks received from the ENISA ad hoc Working Group on Cybersecurity Threat Landscapes suggested to consider the platform element in the analytical framework. For example, the Atlantic Council's Digital Forensic Research Lab (DFRLab) describes the medium through which the disinformation is conveyed, to include open web, social media, and messaging services. https://github.com/DFRLab/Dichotomies-of-Disinformation#platforms.
[12] https://attack.mitre.org/matrices/enterprise/
[13] https://disarmframework.herokuapp.com/

Although in FIMI/disinformation the secondary effect is often speculative, in an attempt to capture the actual intent of an attacker, the events are described in terms of:

- Primary sector/victim/impact
- Secondary sector/victim/impact

Table 2: Example: fake accounts on social media posting critical allegations about a country's government

Categories	Primary	Secondary
Sector	Medias and audio visual	Citizens
Victim	Public	Government/Country
Impact	Political	Social

Concerning the sectors, the framework uses the sectors of Open Cyber Threat Intelligence (Open CTI)[14], since they encompass a wider and hierarchical range of actors – from economic sectors to political parties and citizens – and can more accurately reflect the wide FIMI/disinformation landscape. In addition, it uses the list of essential sectors included in the EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)[15], as well as the recently adopted revised NIS2 Directive[16].

The breakdown of sectors is available on GitHub[17].

The category of "Impact" is broken down as follows:

- Impact
- Financial
- Availability[18]
- Reputation
- Social
- Political

The break-down for the victims is outlined below.

Table 3: Victims - sub-categories and definitions

Victims	Definition
Private sector	Private entities, e.g. companies, industries, etc.
Government / Country	Entities with representative power e.g. ministries or governmental officials

[14] OpenCTI is a product powered by the collaboration of the private company Filigran, the French national cybersecurity agency (ANSSI), the CERT-EU and the Luatix non-profit organization. More information: https://github.com/OpenCTI-Platform/datasets
[15] https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[16] See https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
[17] OpenCTI is a product powered by the collaboration of the private company Filigran, the French national cybersecurity agency (ANSSI), the CERT-EU and the Luatix non-profit organization. More information: https://github.com/OpenCTI-Platform/datasets
[18] Availability can be resource availability, service availability, and/or operation(business) continuity.

Public	Public entities without representative power e.g. hospitals, administrations and citizens
Individual	Single persons

2.3 SEVERITY AND DURATION

At the design stage of the proposed approach, attempts were made to calculate the seriousness of an event based on its duration and its effects on the real world. However, it was noticed that:

- It was difficult to gauge with precision the duration of a FIMI/disinformation event – especially in light of the fact that some events refer to incidents (one-off, unique activities) and others to operations.
- The impact of FIMI/disinformation events would depend in particular on their outreach beyond the initial "information bubble."

As a consequence, it was decided to analyse **duration** independently and to distinguish the effects of a FIMI/disinformation event into **severity** (that is, the reach of a FIMI/disinformation event) and **impact** (that is, the domain affected). The tables below describe the categories of duration and severity, whereas the impact is described in the previous section.

Table 4: Duration – subcategories and definitions

Duration	Definition
Short	The event lasts less than a week
Medium	The event lasts more than a week and less than a month
Long	The event lasts more than a month[19]

Table 5: Severity - sub-categories and definitions

Severity	Definition
1 -Very Low	The incident was shared and/or noticed only within and by the network that launched the incident
2 - Communication Breakout (Low)	The incident was shared and/or noticed beyond the network that launched the incident
3 - Real World Breakout (Medium)	The incident left the scope of communication environments and led to non-harmful actions in the real world (like peaceful demonstrations)
4 - Real World Harm (High)	The incident left the scope of communication environments and led to harmful actions in the real world (i.e. attacks on people, destruction of property, harmful self-medication etc.)

[19] Although this data label refers to events that last longer than one month, it is important to note that FIMI/disinformation events can last years.

2.4 THREAT ACTORS AND MOTIVATION

The classification of threat actors is based on the attribution – technical (TA) or political (PA) – and on whether the entity identified as responsible for the event was a state actor, a non-state actor or a proxy.

Table 6: Threat actor

Threat Actor	Definition
State actor PA	State actor identified with political attribution i.e. through official statements or reports
Non-State actor PA	Non- State actor identified with political attribution i.e. through official statements or reports
Proxy PA	Proxy actor identified with political attribution i.e. through official statements or reports
State actor TA	State actor identified with technical attribution i.a. through statements by victims e.g. platforms, or independent research by civil society
Non-State actor TA	Non- State actor identified with technical attribution, i.a. through statements by victims, e.g. platforms, or independent research by civil society
Proxy TA	Proxy actor identified with technical attribution, i.a. through statements by victims, e.g. platforms, or independent research by civil society
Not officially attributed	No information about attribution
Other	Category not reflected above [free text]

The motivation has been categorised as in:

- Geopolitical
- Disruption
- Manipulation of information[20]
- Ideological
- Monetisation
- Other

2.5 DISARM FRAMEWORK AND MITRE ATT&CK

The DISARM (DISinformation Analysis & Risk Management) framework is designed for describing and understanding the behavioural parts of FIMI/disinformation. The report uses the DISARM Red framework[21], which focuses on FIMI/disinformation creation and dissemination behaviours[22]. The framework is inspired by the structure of the MITRE's ATT&CK ® framework, which is a knowledge-

[20] As explained in section 2.4, the category "Manipulation of information" has been used at the triage stage to identify the events in scope of the report, which all share this motivation. Accordingly, the analysis of section 3 does not include "manipulation of information" among the motivations.
[21] https://disarmframework.herokuapp.com/
[22] The other DISARM framework is called "DISARM Blue", which focuses on disinformation countermeasures. DISARM Blue maps response options to take in reaction to the TTPs outlined in DISARM Red.

base of cyber adversary behaviour and taxonomy for adversarial actions across their lifecycle. The DISARM Red Framework is a useful tool to describe FIMI TTPs. DISARM is born out of the collaborative effort of individuals from the FIMI defender community, which introduced the concepts of kill chain, tactics, techniques and procedures (TTPs) and behavioural fingerprints to the FIMI field. Due to its threat-informed, open-source and community-driven nature, the DISARM framework allows to consolidate all known FIMI TTPs. It also introduces a taxonomy for defenders to speak a common language when describing their findings.

In the present report the DISARM framework is used jointly with MITRE ATTA&CK. MITRE ATT&CK has two parts: ATT&CK for Enterprise, which covers behaviour against enterprise IT networks and cloud, and ATT&CK for Mobile, which focuses on behaviour against mobile devices. The report uses MITRE ATT&CK for Enterprise[23].

Both the DISARM and MITRE frameworks are structured across Tactics, Techniques and Procedures (TTPs). During the initial phase of work on the report it was noticed that mapping events against tactics and techniques using only one of the frameworks was not sufficient to understand both cyber and FIMI dimensions. Hence the report suggests to use uses both frameworks to capture the entire complexity of the events. This is a finding in itself, necessitating better and more in-depth incident reporting both in the cyber and FIMI/disinformation domains and ensuring that the two communities exchange information.

The joint use of the DISARM and MITRE frameworks helps identifying cybersecurity patterns used in support of FIMI/disinformation behaviours and, at the same time, the mapping of FIMI/disinformation patterns against cybersecurity TTPs. By analysing TTPs using only one of the two frameworks, one might overlook TTPs from the other dimension, which could be important insights about the event as well. FIMI/disinformation events often also incorporate a cyber element, whose analysis can assist for the event's attribution, as well as for the identification of indicators of compromise that enable rapid mapping. Conversely, by analysis only cyber TTPs, important elements such as severity and impact cannot be conceptualised and the coordinated nature of such complex events might be missed. The complementarity of the analyses resulting from the combination of these two frameworks brings to more comprehensive threat intelligence. This is especially important in light of hybrid campaigns and the EU's ambition to tackle such threats holistically. Facilitating the joint use of frameworks established for specific domains can significantly boost comprehensive situational awareness and early warning. Sharing insights in an interoperable way between the FIMI/disinformation and cybersecurity domains can lead to quicker and more effective responses, mitigating the severity of harmful activities.

[23] https://attack.mitre.org/matrices/enterprise/

3. TESTING THE FRAMEWORK: ANALYSIS AND TRENDS

This section presents a proof of concept for the joint use of cybersecurity and FIMI/disinformation cases through the analysis of a set of indicative cases. The section showcases the feasibility and potential of the proposed approach, identifies trends and patterns and yields novel insight on the complementary of the FIMI/disinformation and cybersecurity domains, by identifying correlations among them.

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

The events analysed in this report are based on OSINT (Open Source Intelligence) collected by ENISA for situational awareness purposes[24] and are all publicly disclosed. The scope of the collection is global and multi-sectorial. However, events with a direct impact in the EU area are given a priority.

Specifically, the proposed approach is tested against 33 events that have been collected by ENISA in the period from January 2020 until mid-June 2022 and that at a first triage state where identified as motivated by the manipulation of information[25]. It is to be noted that singling out this motivation might not be straightforward. For example: how should a phishing mail with false information luring the receiver to click on a link be considered? In the context of the report, phishing would be analysed only if it contributes to manipulating the information environment, for instance by supporting the compromise of accounts that would facilitate the legitimisation and spread of disinformation.

Another important consideration is that it has not been possible to identify upfront which of the events fell into the definition of FIMI, which outlines many specific features. This is normal since, as reminded throughout the report, the proposed approach is meant to be used by the counter FIMI/disinformation and the cybersecurity communities to improve the description of events, amplify joint situational awareness and, as a result, it is expected to help identifying those that call for EU action with particular attention to FIMI. After the analysis has been carried out it has been noted how not all the events analysed could be considered FIMI, although all of them have been considered as motivated by the manipulation of information (see above). For simplicity, the report refers to the analysed events as **FIMI/disinformation events**.

Finally, one issue that emerged during the analysis is that some **events** referred to **information/cyber incidents** that are part of the same **information operation**[26] and others referred to **information** operations composed by different **information/cyber incidents**. In addition, some **information/cyber incidents** seem to be correlated, raising the question of how they should be counted. For simplicity and being aware of the limitations, the report labels as "**events**" both **information/cyber incidents** and **information operations** and does not group coordinated events into a single one.

[24] In accordance with the EU cybersecurity act Art.7 Par.6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)
[25] As explained in section 2.4, the framework underlying the ENISA Threat Landscape includes among the possible motivations also the category "Manipulation of information". This category has been used to select the events to be analysed in the current report, which are all motivated by the manipulation of information. Accordingly, this category is not reflected in the analysis of motivations in section 3.2.3. Still, it has been included in the description of "Motivations" as it could be used at the triage stage to identify relevant events.
[26] "*Information operation' means planned and coordinated actions and measures used to influence the target audience"* - National Cybersecurity Status Report 2020 – Ministry of National Defence of the Republic of Lithuania

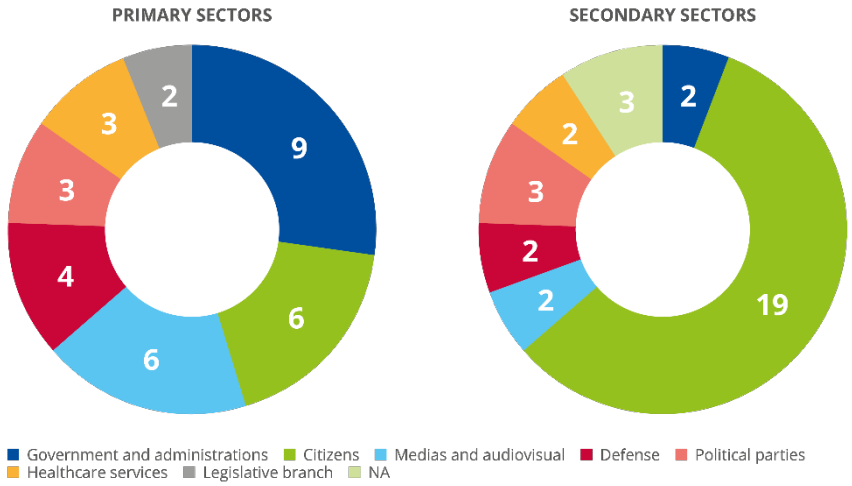
3.2 APPLICATION OF THE PROPOSED APPROACH – DATA ANALISYS

3.2.1 Sectors, victims and impact

As stated in section 2.2, events have primary and secondary sectors, victims and impacts. The graphs below show this duality.

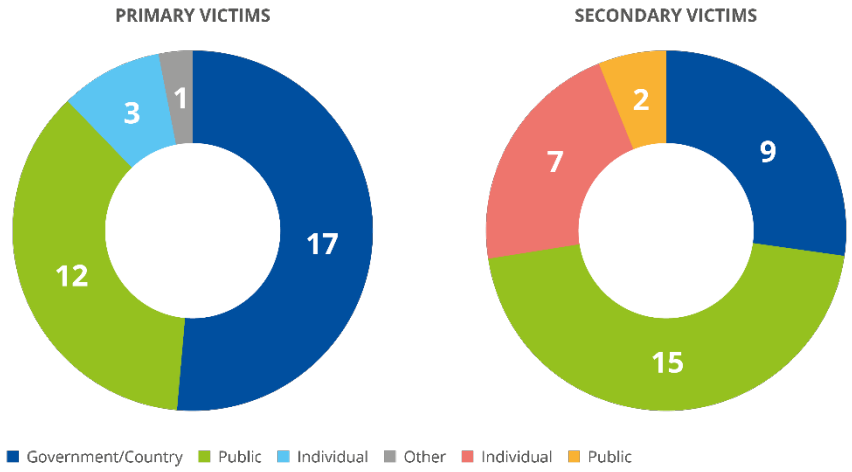
Concerning the sectors, it has been analysed that more than half of the events (18) had a direct impact on actors who are related to different aspects of a State (namely: government and administrations, political parties; defence and legislative branch). In most of cases, citizens have not been impacted directly, but rather as a consequence. They represent the secondary target in more than half (19) of the events. The relevance of the media and audio-visual sector is especially noteworthy. Cybersecurity analysis has a strong focus on critical sectors (e.g. energy or transport), whose disruption, by definition, is particularly serious and addressed by specific legislation (e.g. NIS Directive). Clearly, in the context of FIMI/disinformation, the sector of media and audio-visual is also to be considered as critical.

Figure 1: Primary and secondary sectors



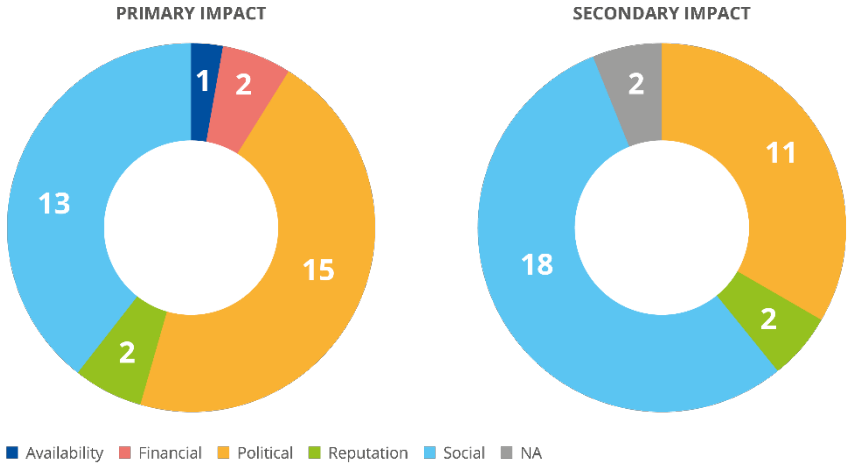
The observations above mirror the ones on the victims, with governments being the primary victims in 17 events and the public and individuals being secondary victims (in 22 cases).

Figure 2: Primary and secondary victims



When the impact is analysed, the results do not differ to a great extent from primary to secondary. In both cases there is a strong focus on social and political impacts (the former more pronounced in the category of secondary impacts).

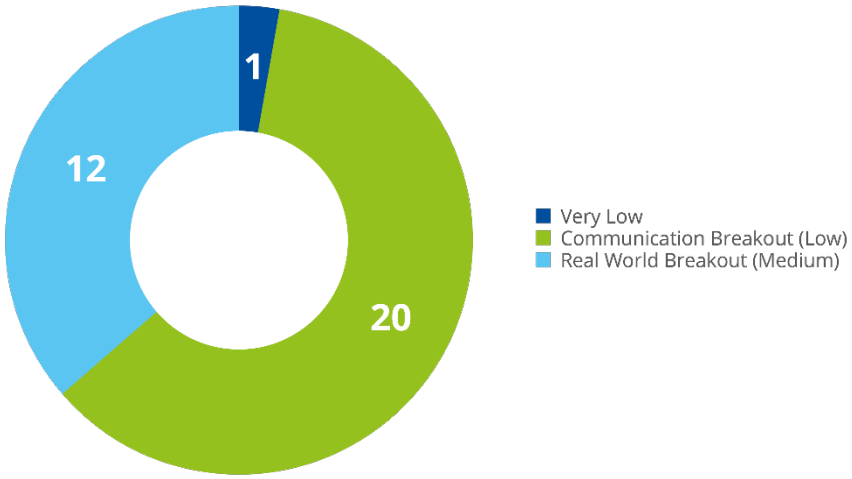
Figure 3: Primary and secondary impact



3.2.2 Severity and duration

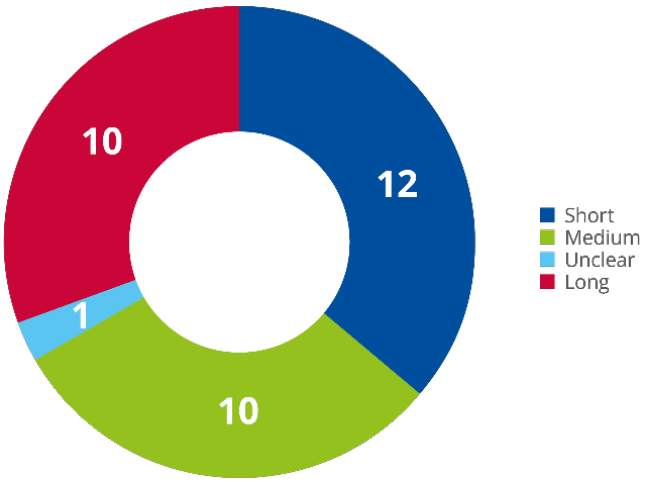
The severity of the great majority of the events analysed is either low or medium, meaning that they were systematically shared/noticed beyond the network that launched the incident (low severity) and left the scope of the communication environment (medium severity), although without leading to prominent actions in the real world.

Figure 4: Severity



Concerning the duration, it is considered based on the reported event (that is, not distinguishing among incidents and operations). Therefore, observations related to duration are made with a low degree of confidence. In particular, while the 10 events featuring a long duration (that is, they lasted more than one month) correspond to operations featuring multiple incidents, it is unclear whether events with a shorter duration are in fact incidents part of an operation extending over a longer period of time.

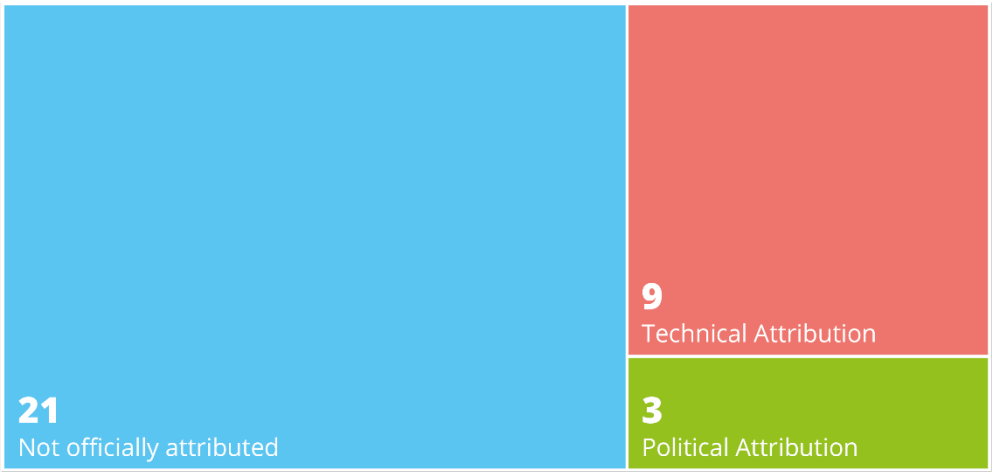
Figure 5: Duration



3.2.3 Threat actors and motivation

The analysis of the threat actors focused on attribution. Not surprisingly, for the great majority of the events (about 2/3), an attribution could not be found and for the remaining events technical attribution seems to be more frequent.

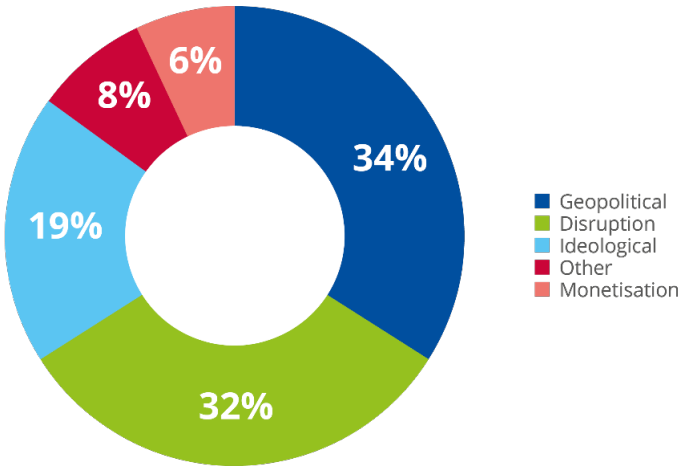
Figure 6: Attribution (number of events)



The analysis showed multiple motivations underlying single events. For example, multiple social media accounts run from a single location and perpetuating a critical narrative with respect to a government might be motivated by ideology, but also by the willingness to disrupt. For this reason, multiple motivations have been associated to single events.

About two-thirds of the motivations identified referred to geopolitics or disruption. The line between disruption, ideology and geopolitics can be blurred at times since disruption can be carried out for ideological and/or geopolitical motives. Therefore, the allocation of an event to a category could be facilitated by a more elaborated definition of motivations. Monetisation has been identified as motivation only in rare cases.

Figure 7: Motivations associated to events



3.2.4 DISARM framework and MITRE ATT&CK

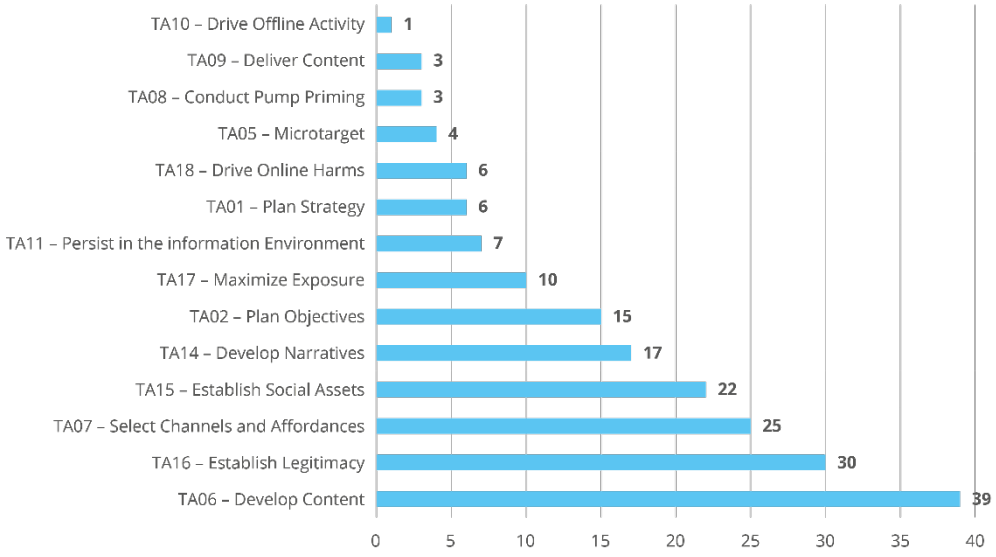
In this section the events have been mapped against both the DISARM and the MITRE ATT&CK tactics with the ultimate goal to identify the FIMI/disinformation tactics (as defined in the DISARM framework) that are impacted the most by cybersecurity tactics (as defined in MITRE ATT&CK). The idea is that, on the ground, the detection of specific MITRE ATT&CK TTP(s) could act as an indicator of a FIMI/disinformation event.

Accordingly, the analysis contained in this section starts with the identification of the most recurrent tactics firstly as per the DISARM framework (sub-section 3.2.4.1) and, secondly, as per the MITRE ATT&CK framework (sub-section 0). Lastly, the analysis unfolds with the joint use of the frameworks, by showing the MITRE ATT&CK tactics and techniques associated to the most recurrent DISARM tactics (sub-section 0). Considerations on the affected assets are also included.

3.2.4.1 DISARM Framework perspective

The table below shows the distribution of the most recurrent tactics according to the DISARM framework. The analysis has been carried out by associating to each FIMI/disinformation event several tactics.

Figure 8: Distribution of FIMI/disinformation tactics according to the DISARM framework



Based on the above, the most recurrent DISARM tactics are displayed in the table below. The most recurrent tactics are those that have been identified at least 10 times[27].

Table 7: Definitions of the most recurrent DISARM tactics

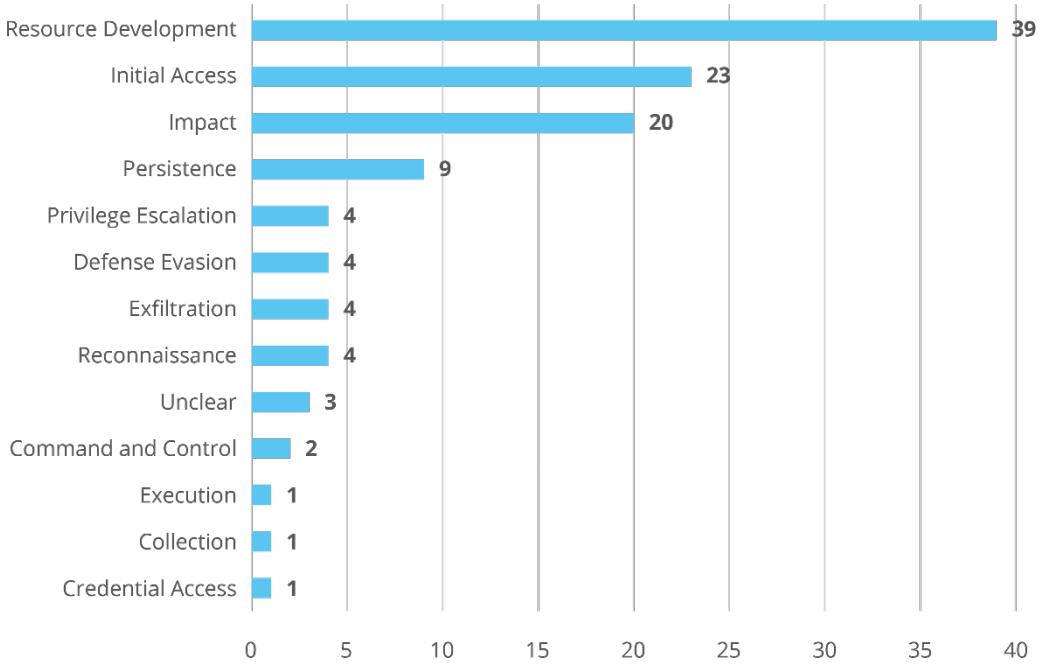
DISARM Tactic	Definition
TA06 - Develop Content	Create or acquire text, images, and other content
TA16 - Establish Legitimacy	Establish assets that create trust
TA 07- Select Channels and Affordances	Selecting platforms and affordances assesses which online or offline platforms and their associated affordances maximize an influence operation's ability to reach its target audience. To select the most appropriate platform(s), an operation may assess the technological affordances including platform algorithms, terms of service, permitted content types, or other attributes that determine platform usability and accessibility. Selecting platforms includes both choosing platforms on which the operation will publish its own content and platforms on which the operation will attempt to restrict adversarial content.
TA15 - Establish Social Assets	Establishing information assets generates messaging tools, including social media accounts, operation personnel, and organizations, including directly and indirectly managed assets. For assets under their direct control, the operation can add, change, or remove these assets at will. Establishing information assets allows an influence operation to promote messaging directly to the target audience without navigating through external entities. Many online influence operations create or compromise social media accounts as a primary vector of information dissemination.
TA14 - Develop Narratives	The promotion of beneficial master narratives is perhaps the most effective method for achieving long-term strategic narrative dominance. From a ""whole of society"" perspective the promotion of the society's core master narratives should occupy a central strategic role. From a misinformation campaign / cognitive security perspective the tactics around master narratives center more precisely on the day-to-day promotion and reinforcement of this messaging. In other words, beneficial, high-coverage master narratives are a central strategic goal and their promotion constitutes an ongoing tactical struggle carried out at a whole-of-society level. Tactically, their promotion covers a broad spectrum of activities both on- and offline.
TA02 - Plan Objectives	Set clearly defined, measurable, and achievable objectives. Achieving objectives ties execution of tactical tasks to reaching the desired end state. There are four primary considerations: - Each desired effect should link directly to one or more objectives - The effect should be measurable - The objective statement should not specify the way and means of accomplishment - The effect should be distinguishable from the objective it supports as a condition for success, not as another objective or task.
TA17- Maximize Exposure	Maximize exposure of the target audience to incident/campaign content via flooding, amplifying, and cross-posting.

[27] It is to be noted that the tactics outlined in this graph represents more than 85% of the total.

3.2.4.2 MITRE ATT&CK Framework perspective

The table below shows the distribution of the most recurrent tactics according to the MITRE ATT&CK framework. The analysis has been carried out by associating to each FIMI/disinformation event several tactics.

Figure 9: Distribution of FIMI/disinformation tactics according to the MITRE ATT&CK framework



Based on the above, the most recurrent MITRE ATT&CK tactics are displayed in the table below. The most recurrent tactics are those that have been identified at least 10 times[28] are: Resource development, Initial access, and Impact.

Table 8: Definitions of the most recurrent MITRE ATT&CK tactics

MITRE ATT&CK Tactic	Definition
Resource Development	Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities. These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access, or stealing code signing certificates to help with Defense Evasion.
Initial Access	Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.
Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data. Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

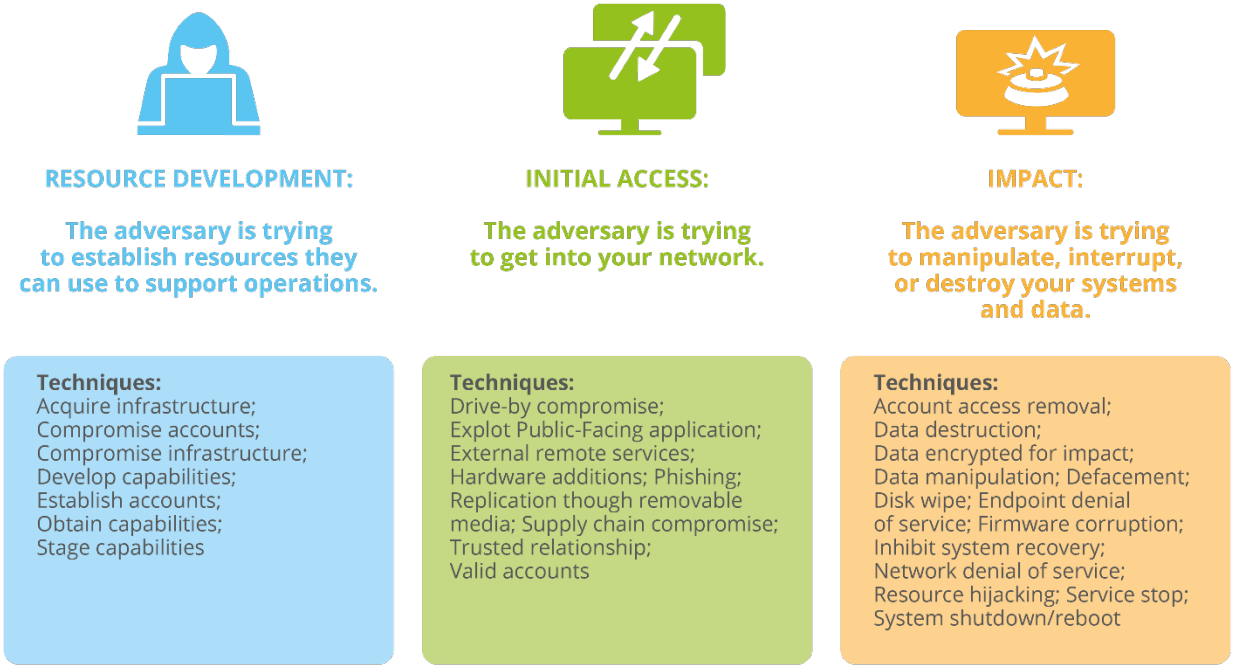
[28] It is to be noted that the tactics outlined in this graph represents more than 70% of the total.

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

Unsurprisingly, when the DISARM and MITRE ATT&CK frameworks are applied jointly, it is noted that the three most recurrent MITRE ATT&CK tactics mentioned above (that is: Resource development, Initial access and Impact) are also the most used *within* each DISARM tactic, as shown in the Annex.

The graphic below shows the definition of the three most recurrent MITRE ATT&CK tactics and of the techniques the framework associates to them.

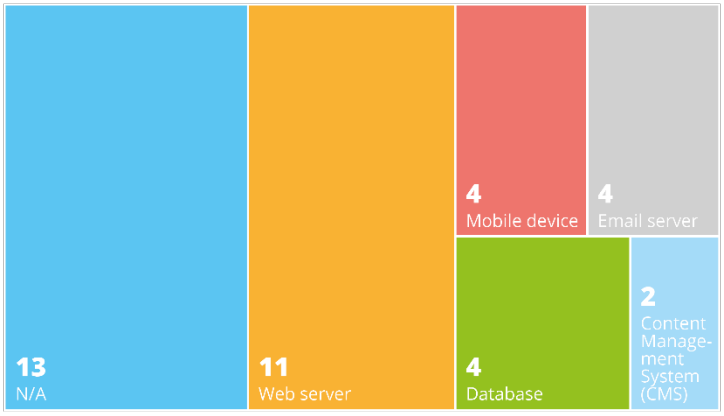
Figure 10: Definition of the three most recurrent MITRE ATT&CK tactics and techniques



It is important to note that these techniques are those associated to the identified tactics by the MITRE ATT&ACK framework i.e. not all of them correspond to the analysed events. Future and more in-depth applications of the approach proposed in this report might carry out a more detailed analysis and dig also into the techniques. This is also due to the quality of the data, often not sufficiently precise to determine the specific technique.

An analysis of the assets impacted has been carried out, although it also suffers from the lack of information as, in most of the cases (13 events out of 33), it has not been possible to understand which asset had been affected by an event.

Table 9: Assets affected by FIMI/disinformation events[29]



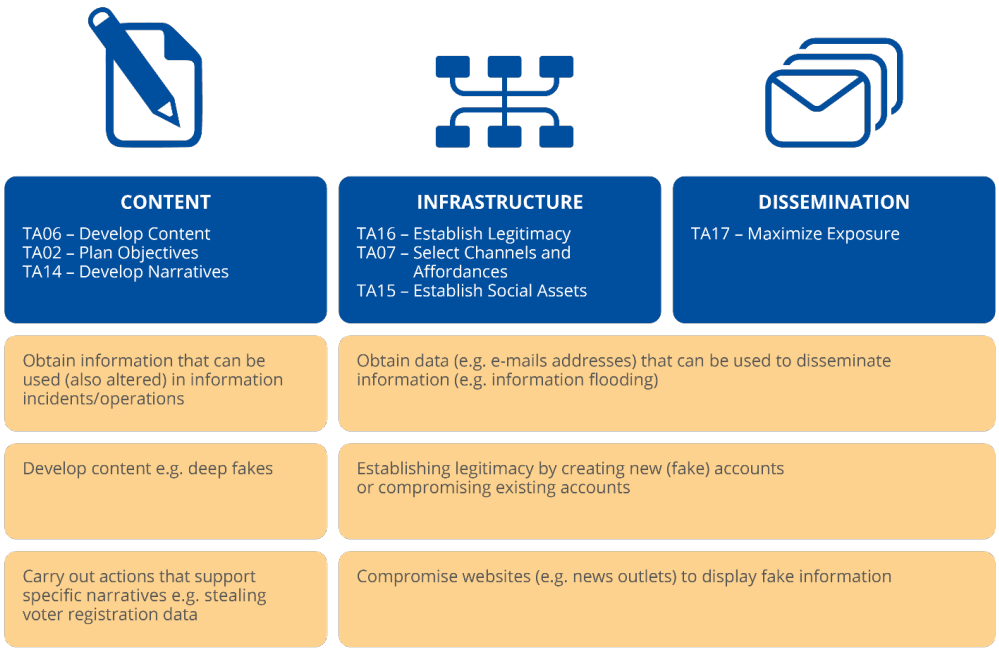
* Each event might be associated to more than one asset

3.2.4.4 The role of cybersecurity

Cybersecurity attacks play an important role in the manipulation of the information environment and, in particular, they provide some of the tools that enable information incidents and operations, especially in terms of content and infrastructure at the initial stages of a FIMI/disinformation event. They also play a role in dissemination, although to a lesser extent.

The graph below conveys a qualitative analysis of the cyber-security activities that have been associated to the most recurring DISARM tactics.

Figure 11: Role of cybersecurity (in orange boxes) across the most recurring DISARM tactics (in blue boxes)



[29] Each event might be associated to more than one asset

4. RECOMMENDATIONS

4.1 TECHNICAL

4.1.1 On the analytical framework

As described in section 2, this report showcases how the interaction between frameworks developed for different domains can lead to enhanced situational awareness. Through the application of both frameworks to specific events, it is possible to:

- Describe FIMI/disinformation creation and dissemination behaviours
- Show the role of cybersecurity (or lack of thereof) in facilitating FIMI/disinformation by identifying the underlying cybersecurity elements
- Expose the manipulative and harmful behaviours the EU wants to prevent, deter and respond to by helping singling out incidents that can be considered as FIMI

Enhance the collective understanding of the kill-chain across the FIMI/disinformation and cybersecurity domains, opening up to new and potential earlier response options While the combination of practices from different domains can be considered overall effective, the implementation of the proposed approach implementation reveals some peculiarities that merit attention and potentially further refinement.

- **Distinction between information/cyber *incidents* and *operations*.** Somewhat differently from the "purely" cybersecurity domain, open-source data about FIMI/disinformation events often cover entire operations encompassing several incidents. Albeit to a lesser extent, some reports refer to coordinated incidents distinctively. This is normal as FIMI/disinformation events often appear as such only after "connecting the dots" of single incidents. However, it would be important to find a common way to report on FIMI/disinformation events that manages to consider both operations and incidents in a consistent way. The difficulty is to reconcile two seemingly different angles. From the cybersecurity perspective, the focus on incidents is especially important as the cybersecurity tactics are likely to change from incident to incident within the same operation. However, from the FIMI/disinformation perspective, elements such as motivation and impact might become evident only by considering operations in their entirety. There is thus a growing need to consider incident reporting initiatives that are prominent in cybersecurity, also in the field of FIMI and foster relevant information sharing mechanisms either voluntarily (for example building on existing or new ISACs) or mandatory (by means of legal instruments, such as NIS2 in the case of cybersecurity).
- **Difficulties in establishing the duration of events**. This aspect partly derives from the previous one. A cybersecurity incident spanning over a few days might have an impact on the information environment that goes way beyond that timeframe. In addition, it might not be always clear what constitutes the "end" of an operation, as opposed to the "temporary pause of an operation". As explained, the proposed approach has been applied in such a way that duration is considered based on the reported event (that is, not distinguishing among incidents and operations), which is sub-optimal. This aspect would probably not be as problematic once a distinction between incidents and operations is made.
- **DISARM vs MITRE: the importance of focusing on DISARM tactics to analyse the cybersecurity component of information events.** The DISARM framework is very good at describing sets of (FIMI/disinformation) incidents that have a common (FIMI/disinformation) goal and are part of the same operation, whereas MITRE is very good at describing single (cybersecurity) incidents, regardless of whether they have the same goal or are part of the same operation. Therefore, it has been found that the most effective way to jointly use of the two frameworks is to analyse the MITRE tactics and techniques at the level of specific DISARM tactics.

- **The primary target (in terms of victims, sectors and impact) is often not the real/main one**. The ENISA Threat Landscape identifies the sectors affected by a cyber-incident, without the need to specify whether the sectors identified are primary or secondary targets. In the case of FIMI/disinformation events, however, it is important to assess whether the directly affected victim/sector/domain (primary) is the actual one or is used only as a means to reach a different target (secondary).
- **FIMI/disinformation events do not necessarily target critical sectors.** The analysis of cybersecurity incidents often focuses on critical sectors as per applicable EU legislation, namely the NIS2 Directive. However, FIMI/disinformation events often target sectors that are not necessarily considered critical (e.g. media) and can have disastrous consequences regardless of the criticality of the sector impacted. The current framework includes both the categories identified by the Open Cyber Threat Intelligence Platform and the NIS Directive. The Open CTI Platform is deemed more appropriate for disinformation events.

4.1.2 On the role of cybersecurity

Based on the above, four areas emerge as important to tackle the manipulation of the information environment from a cybersecurity perspective:

- **The role of cybersecurity seems to be particularly important in establishing attribution**. While most of the events analysed were not attributed (see section 3.2.3), those that had been attributed relied on a cybersecurity analysis. It would be beneficial to create a structured link between technical attribution and FIMI/disinformation.
- **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.** Seam-less cooperation procedure between the cybersecurity and counter FIMI/disinformation communities could yield significant benefits.
- **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.** For example, in many cases the description of the cyber-component was not sufficiently detailed to identify the cybersecurity techniques utilised. As outlined in the ENISA Threat Landscape 2021, more work is needed to better classify cyber incidents related to disinformation and misinformation. On the one hand, a lot of them are classified in other categories given that they are commonly used in complex, hybrid attacks. On the other hand, data concerning FIMI/disinformation does not necessarily dig into cybersecurity aspects. This shows that more cooperation between the cyber and the counter-FIMI community is needed to bring these insights together in a more structured and systematic manner[30].
- **Another limitation has been the comparability of different events, hence reporting needs to be made as coherent as possible.** Incident reporting and information exchange are fundamental components of the lifecycle of response to both cybersecurity and FIMI/disinformation incidents. It would be important to assess how to best integrate cybersecurity and FIMI/disinformation aspects in reporting and information exchange. The use of DISARM in combination with MITRE ATTA&CK could constitute a starting point. Both frameworks take into account the specificities of the respective domains to be able to analyse and describe effectively any activity in either the cyber or FIMI domain. However, it has

[30] Some examples of work in this direction: EUvsDisinfo is a project led by the EEAS that identifies, compiles, and exposes disinformation cases originating in pro-Kremlin media (https://euvsdisinfo.eu/); the open source threat intelligence platform MISP which contains a "galaxy" (a method to express an object that can be attached to events or attributes) on threat actors (https://www.misp-project.org/galaxy.html#_misinformation_pattern); the European Digital Media Observatory that brings together fact-checkers, media literacy experts, and academic researchers to understand and analyse disinformation (https://edmo.eu/edmo-at-a-glance/)

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

become clear that these frameworks should also consider activities that bridge both domains and should be made as interoperable 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.** Awareness raising trainings on cybersecurity are becoming more and more common among organisations e.g. on average, 61% of enterprises provide them (EU average)[31]. Attacks on the governmental/public and media/audio-visual sectors (see section 3.2.1) have been identified as instrumental in obtaining data for the development of content and dissemination and in establishing legitimacy for the dissemination phase. Hence, it is key that awareness raising campaigns are held for these sectors, also flagging the importance of cybersecurity as a means to prevent, deter and respond to FIMI. Awareness raising should also include guidance as to how identify first signals (precursors for a campaign, indicators of a campaign) and then to inform other stakeholders. Moreover, since the more high-level the account compromised is, the more legitimacy it has, it is important that high-profile members of governmental/public and media/audio-visual sectors are aware of this. This aspect might be especially relevant in the context of elections and should therefore be considered to help boost the EU's resilience in view of the 2024 European Parliament election.

4.2 STRATEGIC

FIMI, just like cybersecurity, is a complex, global and ever evolving threat. The vast amount of information attacks prevents any individual defender alone to have a comprehensive and timely overview of the threat landscape. The defender community likewise is highly complex – from governments and international organisations to private industry and civil society as well as academia and journalists, many different stakeholders are involved in tackling FIMI and provide essential contributions to the overall work. Collaboration among defenders is therefore essential. Acknowledging the parallels in the nature of the threat both communities face, we can apply concepts from the cybersecurity community to advance our understanding of FIMI. This includes common definitions, taxonomies and standards such as a data sharing standard, a focus on TTPs, a common methodology and information exchange. Specifically, it is recommended to:

- **Foster mutual exchanges between the cybersecurity and FIMI/disinformation community**. As this report outlines, concepts of cybersecurity can be applied to the detection and analysis of FIMI/disinformation incidents and operations. Existing frameworks, taxonomies, tools, structures and interoperable standards from cybersecurity can be adapted and adopted by the counter FIMI/disinformation community to speed up analytical maturity and interoperability within and beyond the field. Indeed, incident handling and response has been at the core of the cybersecurity community for many years, meaning that procedures and reporting are codified[32]. The behaviour-focussed work on counter-FIMI/Disinformation, instead, is relatively more recent, considering that for many years, the main focus has been laying on "disinformation" and there with the content, not the manipulative tactics. Interoperable, reliable and consistent analytical output by the FIMI/disinformation community can, in return, inform cybersecurity practitioners on new and emerging motivations, targets and threat vectors. Such exchanges can also help disrupt activities that span both domains at an earlier stage.
- **Improve the availability and quality of FIMI/disinformation incident information**. Aggregable and representative information on FIMI/disinformation incidents is so far mostly unavailable. While individual data and research exist and stakeholders do share highly relevant insights, the sector is still underdeveloped compared to the diversity, specialisation and quantity of information shared in the cybersecurity sector. FIMI defenders should consider building on the behaviour (TTP) focus for FIMI detection and analysis. Organisations maintaining FIMI SOCs can drive the development or adoption of commonly shared

[31] Source: Eurostat ("*Enterprises make persons employed aware of their obligations in ICT related issues*" – 2019 data) - https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do
[32] For example, one important lesson from the "traditional" cybersecurity analysis is to avoid the abundance of threat actors/campaign naming.

frameworks and standards inter alia in voluntary vehicles like Information Sharing and Analysis Centers (ISACs) for FIMI.

- **Adopt and adapt standard information formats for sharing FIMI/disinformation intelligence**. The more structured information about incidents available, the higher each investigator's effectiveness. Building again on good case practices from cybersecurity, the FIMI community can adopt and adapt standard information formats, such as STIX[33], the Standard Threat Information Expression language, to move beyond information sharing by written reports. DISARM TTPs are already available as attack patterns in STIX format; other STIX objects help to easily and comprehensively communicate important information of who did what to whom, when, how and why. Existing STIX objects like threat actors, intrusion sets, observables, vulnerabilities, identities etc. can already be used to communicate the majority of relevant FIMI information. With standardised threat exchange formats automation can be brought into the fight against FIMI and a shared threat intelligence knowledge base could be established. With processes and approaches developed in cybersecurity, the gap between well-resourced attackers and a decentralised but collaborative defender community could be narrowed. By ridging cybersecurity with FIMI analyses, as defenders we have one additional tool of threat intelligence at our disposal to better protect against relevant threats.

4.3 POLICY

Recent EU policy initiatives, such as the Cyber Resilience Act (CRA)[34], the Digital Operational Resilience Act for the financial sector (DORA)[35], Digital Services Act (DSA)[36], Digital Markets Act (DMA)[37], Artificial Intelligence Act (AI)[38], etc. rank cybersecurity high on the agenda across other dimensions compared to strictly defined sectors. Likewise, the Code of Practice on Disinformation (CoP)[39], European Democracy Action Plan (EDAP)[40], the DSA and the Strategic Compass for Security and Defence[41] as well as the European Media Freedom Act (EMFA)[42] highlight the fundamental threat that FIMI poses. FIMI, as outlined in this report, does not necessarily target 'critical sectors', but corrodes the very basis of our democracy and security, by targeting i.a. society at large. Cybersecurity, FIMI and hybrid threats permeate all aspects of our daily lives and thus future policy initiatives should consider these aspects in relevant impact assessment. This leads to the following recommendations:

- The EU Institutions have expert teams dealing with FIMI and cybersecurity respectively, both from a policy and an operational perspective. **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**. Based on the proposed common definition for FIMI and the existing scope of the cybersecurity community, trainings on applying to analytical frameworks in an interoperable way, building respective processes etc. should be supported. Politically, the EU has committed in the Strategic Compass to build a FIMI Data Space, to enhance the EU's posture vis-à-vis FIMI threat actors. This could, based on previous points, be in the shape of an Information Sharing and Analysis Center (ISAC). Exploratory work on this has already started in 2021 in the EEAS, in close exchanges with relevant stakeholders from governments, civil society and private industry. Such a FIMI ISAC should be set up in a timely manner and should be discussed with stakeholders from the

[33] See https://stixproject.github.io/
[34] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[35] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595
[36] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[37] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN
[38] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206
[39] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
[40] https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en
[41] https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en
[42] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5504

cybersecurity community, to ensure the FIMI ISAC is interoperable with existing structures in the cybersecurity domain.

ANNEX

The table below shows, for each of the most relevant DISARM tactics, the top-3 MITRE techniques.

DISARM Tactic	Top 3 MITRE tactics	
TA06 - Develop Content	Resource Development	52
	Impact	25
	Initial Access	14
TA16 - Establish Legitimacy	Resource Development	43
	Initial Access	21
	Impact	17
TA 07- Select Channels and Affordances	Resource Development	33
	Initial Access	13
	Impact	9
TA15 - Establish Social Assets	Resource Development	28
	Impact	15
	Reconnaissance	6
TA02 - Plan Objectives	Resource Development	26
	Impact	8
	Initial Access	7
TA14 - Develop Narratives	Resource Development	15
	Initial Access	8
	Impact	7
TA17- Maximize Exposure	Resource Development	16
	Impact	8
	Initial Access	5

TP-08-22-329-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-606-4
DOI: 10.2824/7501