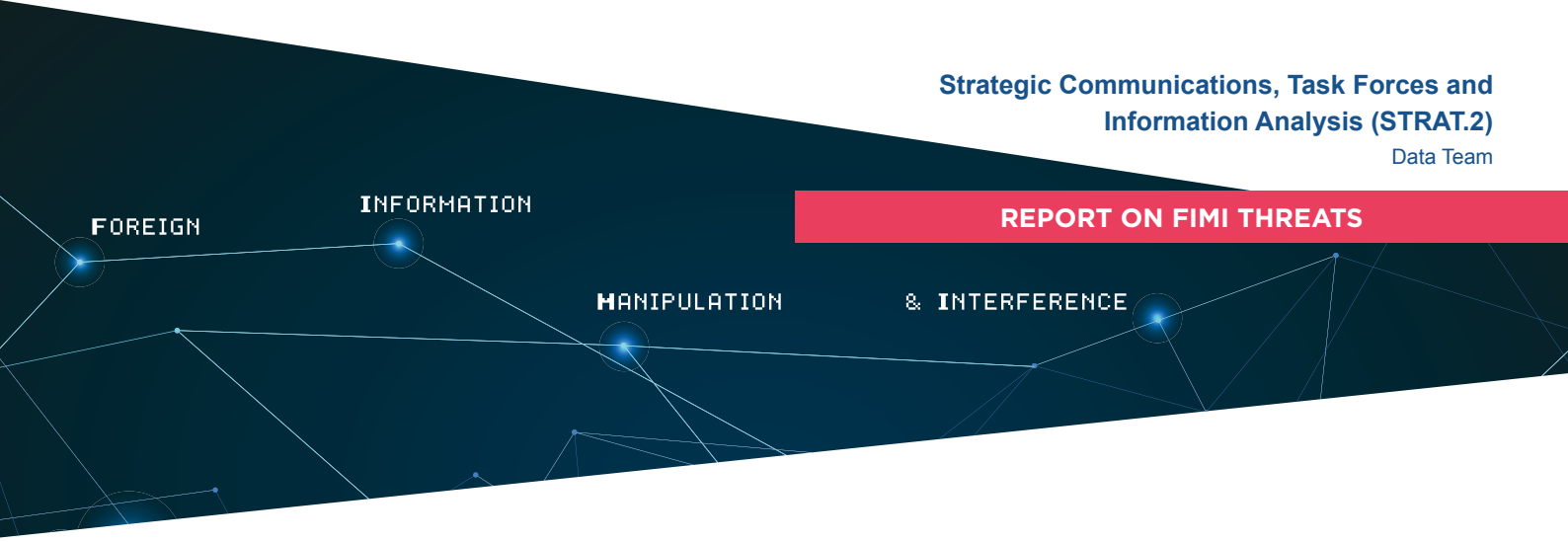
Strategic Communications, Task Forces and
Information Analysis (STRAT.2)
Data Team



REPORT ON FIMI THREATS

1st EEAS Report on Foreign Information Manipulation and Interference Threats

Towards a framework for networked defence

February 2023

European Union
EXTERNAL ACTION

TABLE OF CONTENTS

Glossary 4

Executive Summary 5

1 Introduction 7
Encouraging a Community-Wide Conversation on Best Practices 7
Scope, Limitations, and Caveats 8

2 Focus on Key FIMI Actors 9

3 Pilot Analysis on EEAS Priority Actors and Issues in 2022 11
(Threat) Actors 12
Presumed Objectives 12
Behaviour 13
Tactics, Techniques, and Procedures (TTPs) 13
Content 17
Timeline of Events 17
Narratives 19
Degree 20
Composition of the Threat Actor Media Ecosystem 20
Threat Actors' Infosphere 21
Tools: Distribution of Content 22
Languages 22
Targets 23
Effect 24
Course of Action 24

4 A Behaviour-Centred Problem Definition:
Introducing the Notion of Foreign Information Manipulation and Interference (FIMI) 25
The "Kill Chain" Perspective on FIMI: Expanding the countermeasures toolbox 25
Threat Analysis vs. Disruptive Responses 26

5 An Analytical Framework for FIMI Threat Analysis 27
Analysis Cycle: Establishing a Strategic and Self-Reinforcing Workflow 28
DISARM Framework: A Community-Driven Taxonomy of TTPs 29
Towards a standardised Data Format for Threat Information Sharing 30

Conclusion 32

Recommendations 33

References 34

GLOSSARY

Term	Explanation
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 processed. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory.[1]
Disinformation	Verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security.[2]
Misinformation	Misinformation is false or misleading information shared without harmful intent, though the effects can be still harmful.[3]
Strategic Compass	The Strategic Compass, adopted in March 2022 by the Council, sets out a plan of action for strengthening the EU's security and defence policy by 2030. The objective of the Strategic Compass is to make the EU a stronger and more capable security provider. One of the aspects covered in terms of security policy is the development a Foreign Information Manipulation and Interference Toolbox.[4]
TTP(s)	In the context of FIMI, "Tactics, Techniques, and Procedures" are patterns of behaviour used by threat actors to manipulate the information environment with the intention to deceive. Tactics describe operational goals that threat actors are trying to accomplish. Techniques are actions describing how they try to accomplish it. Procedures are the specific combination of techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different threat actors.
Incidents	A FIMI incident is an action perpetrated by one or more threat actor(s) pursuing specific objectives and carried out with the intent to deceive. It is composed of a combination of observables and TTPs. Multiple related incidents can be part of a campaign.
Observables	Observables are concrete elements relevant to understand how an incident unfolded – such as a tweet, a video on YouTube or an article on a website. Observables can be represented via the URL under which they were found or as files.
DISARM	Disinformation Analysis and Risk Management[5] is an open-source framework designed for describing and understanding the behavioural parts of FIMI/disinformation. It sets out best practices for fighting disinformation through sharing data & analysis, and can inform effective action. The Framework has been developed, drawing on global cybersecurity best practices.[6]
STIX	The Structured Threat Information Expression (STIX™) is a data format used to encode and exchange cyber threat intelligence (CTI). It can also be used to share insights on FIMI incidents, by breaking them down into their different constitutive elements into the STIX format.[7]
Kill Chain	The Kill Chain is a model breaking down multiple stages of an attack perpetrated by a malign actor, allowing analysts to predict, recognize, disrupt or prevent the attack. It is originally a military concept that has been further adapted for cybersecurity and can be applied to FIMI too.
ISAC	Information Sharing and Analysis Centres are trusted entities to foster information sharing and good practices about threats and their respective mitigation. In the context of a FIMI-ISAC, the purpose is to pool insights from the many organizations that expose manipulative activity using common frameworks and standards.

EXECUTIVE SUMMARY

This first edition of the report on Foreign Information Manipulation and Interference threats is informed by the work of the European External Action Service's (EEAS) Stratcom division[8] in 2022. It is the first of its kind and can be seen as a pilot project. It applies a novel framework developed by the EEAS, based on best case practices of the FIMI defender community, to a first **sample of 100 FIMI incidents detected and analysed between October and December 2022. It therefore does not intend to give a comprehensive overview of FIMI in general or of a specific actor, but highlight how the existing analysis can be enhanced through this approach. In this report the EEAS uses best case practice methodology to allow for informed judgements of ongoing FIMI activities, actors and threat levels. It is therefore a useful tool to support informed and analysis based policy choices**. The main findings of this report, based on the samples used, are:

- **Russia's full-scale invasion of Ukraine dominates observed FIMI activity.** Ukraine and its representatives have been the direct target of 33 incidents. In 60 out of 100 incidents, supporting the invasion was the main motivation behind the attack.
- **Diplomatic channels are an integral part of FIMI incidents.** Russia's diplomatic channels regularly serve as enablers of FIMI operations. They are deployed across wide range of topics. China also uses diplomatic channels, mostly targeting the US.
- **Impersonation techniques become more sophisticated.** Impersonations of international and trusted organisations and individuals are used by Russian actors particularly to target Ukraine. Print and TV media are most often impersonated, with magazines seeing their entire style copied.
- **FIMI actor collusion exists but is limited.** Official Russian actors were involved in 88 analysed FIMI incidents. Chinese actors were involved in 17. In at least 5 cases, both actors engaged jointly.
- **FIMI is multilingual.** Incidents do not occur in just one language; content is translated and amplified in multiple languages. Incidents featured at least 30 languages, 16 of which are EU-languages. Russia used a larger variety of languages than Chinese actors but 44% of Russian content targeted a Russian-speaking populations, while 36% targeted English-speaking populations.
- **FIMI is mostly intended to distract and distort.** Russia (42%) and China (56%) mostly intend to direct attention to a different actor or narrative or to shift blame ("distract"). Russia attempts to change the framing and narrative ("distort") relatively more often (35%) than China (18%).
- **FIMI remains mostly image and video based.** The cheap and easy production and distribution of image and video material online makes these formats still the most commonly used.

The report contributes to the implementation of the Strategic Compass' call for a FIMI Data Space.

The EEAS aims to provide the FIMI defender community with a proof-of-concept for a common framework that enables mutual sharing of complex insights in a timely fashion and at scale. This is done to **create a common understanding and formulate a collective, systematic response to FIMI**.

Disclaimer: The empirical data analysed in this report represents a limited time-period in 2022 and reflects patterns seen in known outlets related to **overt** Foreign Information Manipulation and Interference (FIMI) **or independently attributed operations** by selected actors and on priority issues of the EEAS. The evidence presented in this report serves illustrative purposes and should **not be used to draw conclusions about general trends in FIMI**, as they only reflect a limited subset of threat actors activity.

“We have to focus on foreign actors
who intentionally, in a coordinated manner,
try to manipulate our information environment.
We need to work with democratic partners around the world
to fight information manipulation by authoritarian regimes
more actively. It is time to roll up our sleeves
and defend democracy, both at home
and around the world.”

Josep Borrell, High Representative / Vice-President.

1 INTRODUCTION

For as long as people have tried to manipulate the information environment through disinformation and other tactics, people have tried to detect and counter it. Analysis of foreign information manipulation and interference (FIMI), including disinformation has been conducted by individuals, researchers, civil society organisations and governments. More recently, social media platforms and online service providers have had to step up their work to protect their platforms from such manipulation. The challenge is global, complex and ever evolving. To protect universal values, democracy, freedoms and societies, a diverse range of actors has emerged who try to detect, understand and respond – **the defender community**.

Russia's strategic and coordinated use of FIMI in its war of aggression against Ukraine focussed the attention of the defender community, and saw an unprecedented effort to use open-source intelligence to expose Russia's efforts to manipulate global discourse and opinion. It has also underlined how important cooperation between these stakeholders is; **a comprehensive, timely and shared understanding of the threat can lead to effective action denying FIMI its intended effect**. This work to collect evidence, to understand the mechanics behind FIMI and share insights forms the basis for effective and appropriate responses taken by every FIMI defender in civil society, private industry and governments.

Whilst sharing insights contributed significantly to our collective understanding of and resilience to FIMI, both the scope and richness of these insights have grown alongside the threat. **How can we thus aggregate and share complex insights timely and at scale to create a common understanding and formulate a collective, systematic response to the problem?**

The EEAS has continued to raise awareness of FIMI threats through its public reporting, via the EUvsDisinfo website as well as dedicated reports, such as the public reports on COVID-19 disinformation. Under the leadership of the High Representative of the EU for Foreign Affairs and Security and Vice-President of the European Commission (HR/VP) Josep Borrell, the EEAS has built on these experiences and continued to sharpen its capabilities to identify, analyse and assess FIMI in order to facilitate more targeted and effective responses to FIMI. This report on FIMI threats proposes a conceptual foundation to tackle this challenge to fully realise a whole-of-society response to FIMI including disinformation. Independent of the FIMI actor, language, or location of the threat activity, **this framework can accommodate all relevant insights, deliver them to FIMI defenders community and enable a wide array of countermeasures** based on our collective observations.

As such, the report responds to the call by the 2020 European Democracy Action Plan to propose a "*Common Framework and Methodology to systematically collect evidence on FIMI incidents*"[9] and can serve as orientation to deliver on the *2022 Strategic Compass for Security and Defence*. It sets out to "*create an appropriate mechanism to systematically collect data on incidents [of Foreign Information Manipulation and Interference], facilitated by a dedicated Data Space.*" Such a Data Space aims to "*strengthen our ability to detect, analyse and respond to the threat, including by imposing costs on perpetrators.*"[10]

ENCOURAGING A COMMUNITY-WIDE CONVERSATION ON BEST PRACTICES

In June 2022, Carnegie's Partnership for Countering Influence Operations (PCIO) held a workshop during which it convened a group of high-level experts from civil society, industry, and government to take stock of best practices in the FIMI analyst community.[11] While there was broad agreement on what was needed, the exercise was also sobering in the sense that there is a **lack of agreed upon definitions and analytical standards for analysing and reporting on FIMI**. Through this report, the EEAS aims to support the defender community by sharing good case practices to foster a broad conversation on how to move forward. To do so, this report is divided into three sections outlining our proposal:

- **Section 1:** Presentation of a pilot FIMI threat analysis by the EEAS on priority actors and issues in 2022, according to the proposed framework.
- **Section 2:** Introduction of a behaviour-first approach to FIMI detection and analysis, as well as the linked "Kill Chain" perspective on analysing, anticipating and disrupting threat actor behaviour.
- **Section 3:** Sharing of a comprehensive analytical framework covering a self-reinforcing investigative workflow, a taxonomy for threat actor behaviour, and the development of data standards for threat indicators.

The whole-of-society approach is a key element in the EEAS' work to prevent, deter and respond to FIMI. Therefore, we conceive of the development of best practices as a community-driven process; we offer our conceptual

perspective and analytical framework, as a (possible) starting point for a constructive conversation within the defender community. The EEAS' goal is to **facilitate and contribute to the creation of an open source, decentralised and interoperable framework that increases the efficiency of sharing threat insights** between the different stakeholders involved in FIMI analysis and disruption.

SCOPE, LIMITATIONS, AND CAVEATS

Importantly, due to the EEAS mandate to identify and analyse *Foreign* Information Manipulation and Interference and our current priority focus on Russia and China, this **report specifically covers overt FIMI activity or such that can be attributed** to either of these two state actors. This specialisation of the EEAS' work therefore offers targeted insights into these activities which are to be understood as part of the broader threat landscape. The EEAS' analytical framework however is applicable to other regions and actors as well as foreign and domestic analyses due to its actor-agnostic design and is thus addressed at all stakeholders regardless of their respective focus.

The **proposed framework could then enable collaboration and interoperability between analytical teams** mandated to investigate information manipulation in different regions and from different actors. Additionally, it could be applied to understand both foreign and domestic activity. The latter is a crucial advantage as these two spheres often intersect and need to be seen together to properly assess the threat.

2 FOCUS ON KEY FIMI ACTORS

Raising awareness of how FIMI works as well as reporting the latest trends and developments contribute to increasing resilience against the threat in the public. Therefore, in addition to information sharing with partners, the EEAS has been leading on developing the EU's response to FIMI and publicly reporting on Russian FIMI activities since 2015, inter alia via the EUvsDisinfo campaign[12]. With the COVID-19 pandemic, we have also seen China as an emerging and willing FIMI actor[13] and provided insights via dedicated reporting on COVID-19 disinformation. Only by consistently observing and documenting these activities can we understand and illustrate their vast scope, manipulative nature and harmful consequences. It is the entirety of these observations that paints a full picture of the threat and allows us to formulate effective and targeted responses from the short to the long term, from countering individual attacks to closing vulnerabilities and increasing our collective resilience.

Below, we will first briefly summarise what we know on two key FIMI actors from analysis by the EEAS across the last year. Following that, we will outline how these observations can be shared and combined where possible to inform a broad toolbox of countermeasures. In light of the EEAS work to develop the EU FIMI Toolbox to prevent, deter and respond to the threat, these insights are key to understand how to further enhance the instruments at our disposal.

For years, **Russia** has been using the whole playbook of information manipulation and interference, including disinformation, in an attempt to sow divisions in the societies, denigrate democratic processes and institutions and rally support for its imperialist policies. Russia's full-scale invasion of Ukraine on 24th February 2022 has shown, again, the wide spectrum of tactics, techniques and behaviour (TTPs) used in the information environment, while building mostly on well-known disinformation narratives.

Ukraine has been the first target of Russia's FIMI operations. The invasion is a culmination of Russia's years-long information manipulation and interference seeking to undermine the sovereignty and territorial integrity of Ukraine. Nearly all disinformation narratives used by the Kremlin to justify and mobilise domestic support for the invasion can be traced back to 2013-2014 and the Euromaidan protests, in the context of which the Kremlin sought to portray Ukraine as a "Nazi state", a "failed state" and "not a state at all". Pro-Kremlin media have been preparing the soil for the military invasion for years.

Pro-Kremlin outlets have also been instrumental in justifying and obfuscating war crimes and atrocities committed by Russian soldiers in Ukraine. Further enhanced by the Russian losses on the battlefield, hate speech and incitement to genocide became a regular occurrence in Russian outlets, both offline and online. Narratives supporting the war permeate not just political life and news, but also entertainment content.

On the international scene, the Kremlin has been using its information manipulation playbook in attempts to undermine international support for Ukraine. Above all, the goal is to sow doubt about who the aggressor is, hence the focus on disinformation narratives accusing NATO and particularly the US of attempts to encircle and contain Russia via Ukraine. Another goal of Russia is to break the international resolve to condemn the war and impose costs on Russia for its violation of international law. Additionally, through its proxies and manipulative behaviour on social media, pro-Kremlin actors seek to exacerbate and exploit controversial issues: migration and refugees; cost of living; energy prices. Information manipulation and interference, including disinformation targeting international audiences have been instrumental in the Kremlin's attempts to weaponise hunger and energy.

There is no longer any distance between the Kremlin's diplomatic and FIMI arms. In further attempts to sow discord, official social media accounts of Russia's diplomatic representations have been acting as a coordinated amplification network for disinformation narratives, and are now fully integrated into the wider FIMI ecosystem. Russia is also exploiting its presence in diplomatic fora to amplify and legitimise disinformation claims about Ukraine. In further efforts to confuse and distract, Russian diplomatic social media accounts have also been promoting disinformation narratives portrayed as fact-checking.

Inside Russia, the information manipulation and censorship pursued by the Kremlin enabled and continues to fuel the war against Ukraine. Information manipulation and disinformation go hand in hand with the censorship and destruction of independent media. The Kremlin's iron grip on the information environment in Russia is crucial for the Kremlin to ensure the absence of any meaningful domestic opposition to the war. Russia is moving to a state of total propaganda, where the war is presented as an existential fight to defend Russia.

China is a multifaceted FIMI actor with an arsenal that is diverse and includes various tactics. Its activities range from benign – public diplomacy – to clearly illegitimate – intimidation and harassment of critical voices with the aim of suppressing information also outside of its borders. Different elements are often used in combination and can be connected to other forms of interference, for example economic coercion. Over the past few years there has been a widening of Chinese tactics including the repeated spreading of conspiracies by Chinese diplomats, officials and state-controlled media.

When it comes to FIMI activities on international social media platforms, China is a proven FIMI actor, with the first takedown of a disinformation network attributed to the Chinese state in 2019 on Twitter and Facebook. There is also evidence of China's widening use of paid social media influencers with undisclosed connections to Chinese state-controlled media or other structures, to counter criticisms of China's human rights issues and reshape narratives on topics like Xinjiang.

However, China's FIMI activities do not only focus on propagating its own message, but also on suppressing competing voices or messages that would undermine China's official narrative.

Over the years, China has been building its presence in the global information environment, including increased worldwide presence of its state-controlled media. China has been seen using both its own global media footprint and economic leverage over other outlets to influence media coverage, while at the same time heavily restricting reporting by foreign correspondents in China.

While building up its messaging machine, China has made systematic efforts to suppress competing and potentially critical stories about itself, using a wide range of often covert tactics, including intimidating and harassing individuals, also targeting overseas Chinese communities. This dual nature of Chinese activities is significant.

Worries about exporting of Chinese censorship policies have accompanied the global spread of Chinese online platforms. Research has found that users of Chinese platforms like WeChat can still be subject to Chinese online censorship, even when they are physically located outside of China.

When it comes to interactions with other FIMI actors, Russia's war of aggression against Ukraine has provided further evidence of China's and Russia's convergence in the information environment. Chinese state-controlled media and official social media channels have amplified selected pro-Kremlin conspiracy narratives, for example on alleged US military biolabs in Ukraine. On several occasions, Chinese state-controlled outlets have also provided a platform for sanctioned Russian media outlets. The EEAS has identified a number of incidents of disinformation content moving between the Chinese and Russian online FIMI ecosystems, with content created by one actor being amplified by the other.

3 PILOT ANALYSIS ON EEAS PRIORITY ACTORS AND ISSUES IN 2022

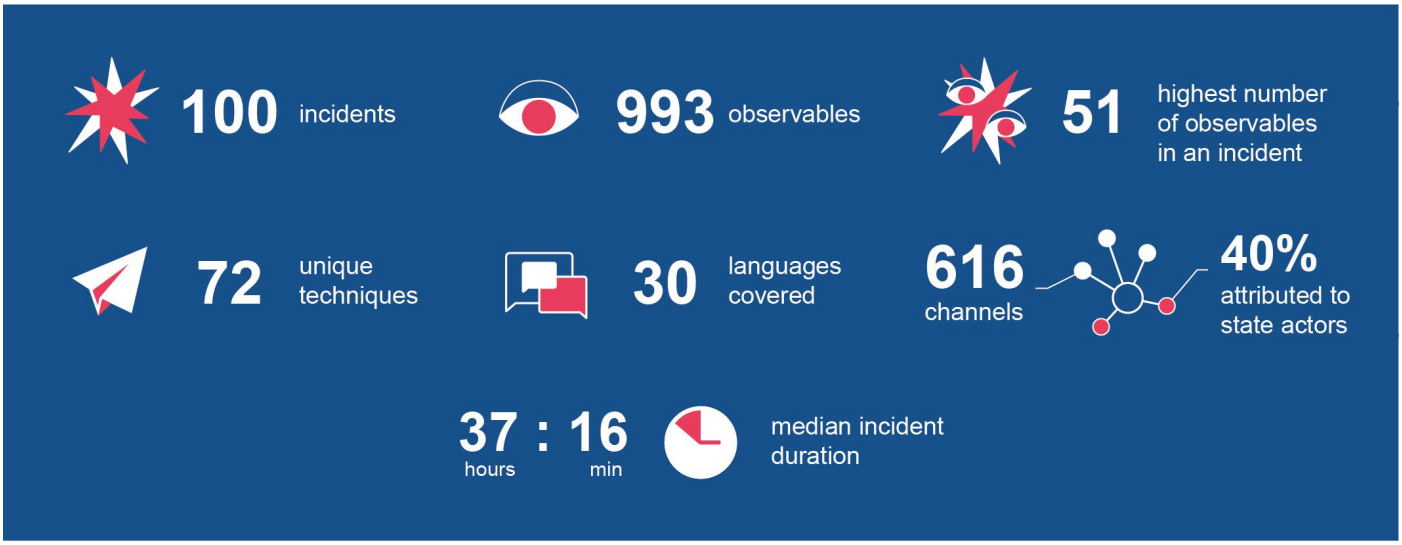


Figure 1 Key figures of findings across 100 FIMI incidents.

The following analysis is **based on 100 FIMI cases (incidents)** continuously detected and analysed between the 1st of October and 5th of December 2022. This report covers Russia and China as FIMI actors. The analysis only considered FIMI incidents in which attributed digital media channels played a significant role in either seeding, relaying or amplifying content. **The Russian ecosystem was involved in 88 cases, while Chinese official channels were reported active in 17 cases.**

In order to investigate and document the incidents, a total of 993 observables (evidence) were found. These figures show that an average incident was usually composed of about 10 observables. However, threat actors can intensify the seeding and spreading of observables in cases of topics particularly relevant to them. Our dataset includes one incident featuring 51 observables (this *excludes* retweets and alike).

According to the threat actors' interests, **FIMI activities targeted multiple geographical locations**. The collection of incidents covers content in 30 languages, including 16 EU languages (BG, CZ, DE, DA, EL, EN, ES, FR, IT, LV, LT, NL, PL, PT, RO, SV).

The majority of the incidents cover FIMI activities in relation to Russia's invasion of Ukraine.

One new insight made possible by a standardised analytical approach was the expected duration of an incident. **The execution phase of each incident** – spanning the time from the publication of the first observable to the last relevant push during the amplification phase – **had a median duration of 37 hours**.

The state media ecosystems of China and Russia operated jointly in 5 incidents, mainly related to anti-Western content. In all of these incidents, threat actors produced collages of pictures or cartoons accusing the US, denigrating EU member states, blaming the EU or questioning the efficiency of sanctions imposed on Russia. In all these cases, the content emerged from Chinese diplomatic accounts and state-controlled channels. Later, their Russian counterparts reused the same observables (in some cases, even translated them into Russian).

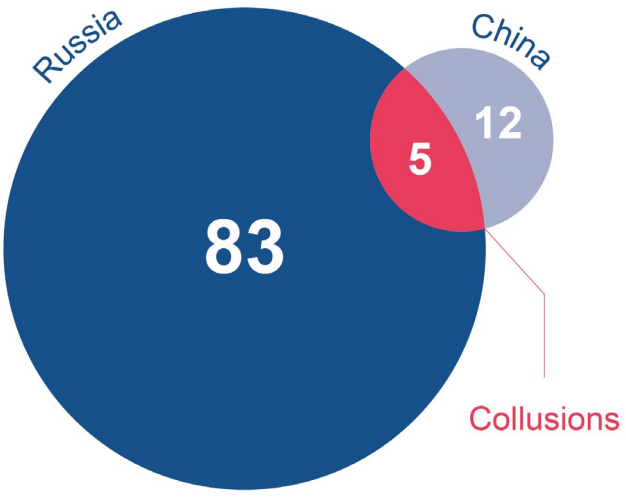


Figure 2 Number of incidents per Threat Actor

(THREAT) ACTORS

Presumed Objectives

What does a threat actor want to achieve with their FIMI activity? To identify potential patterns, we assigned presumed objectives to FIMI incidents. By attaching a presumed objective to each of the 100 incidents we are able to assess if and how threat actors tailor their manipulation techniques according to what motivates their activity. The presumed objective may be identified based on the analysis of the observables and the TTPs, as well as the promoted content.

For this, the 5D (Dismiss, Distort, Distract, Dismay, Divide)[14] classification was used.

- **Dismiss:** to push back against criticism, deny allegations and denigrate the source;
- **Distort:** to change the framing and twist and change the narrative;
- **Distract:** to turn attention to a different actor or narrative or to shift the blame;
- **Dismay:** to threaten and scare off opponents;
- **Divide:** to create conflict and widen divisions within or between communities and groups.

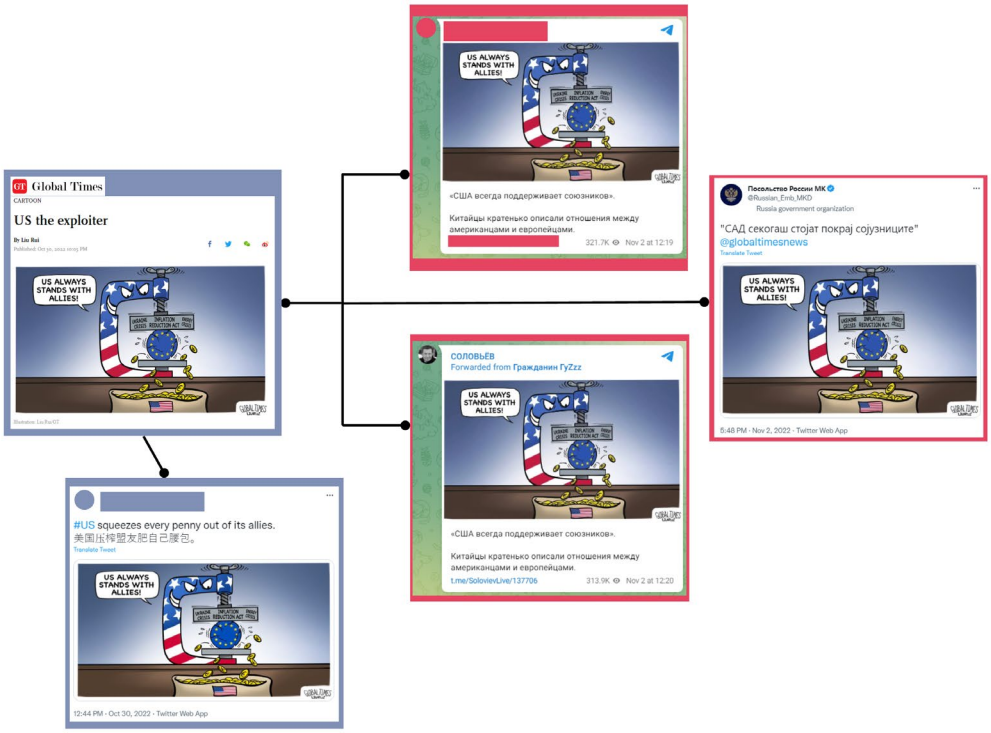


Figure 3 Cartoon produced by Chinese Global Times and amplified by Russian attributed channels

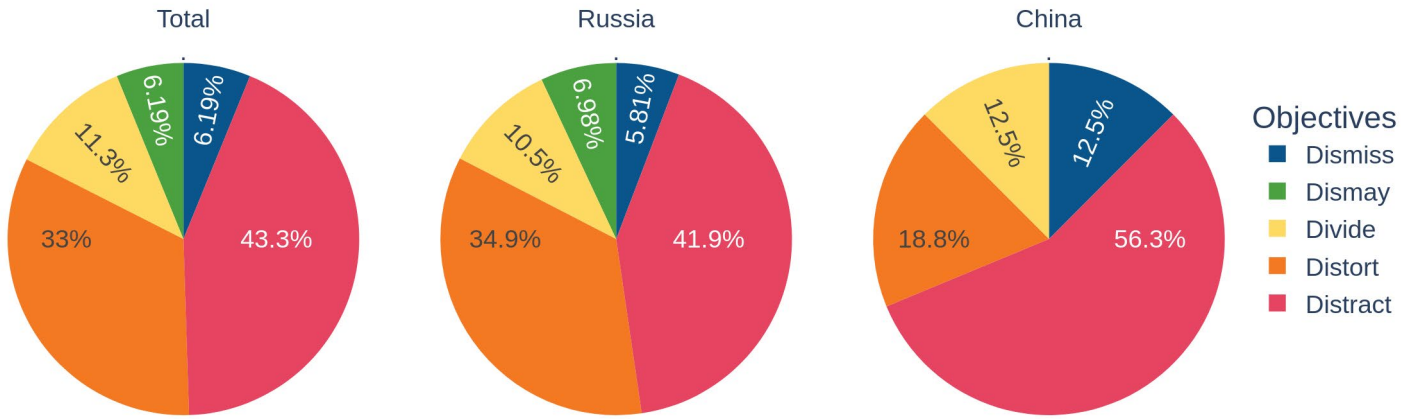


Figure 4 Distribution of presumed objectives overall and per Threat Actor

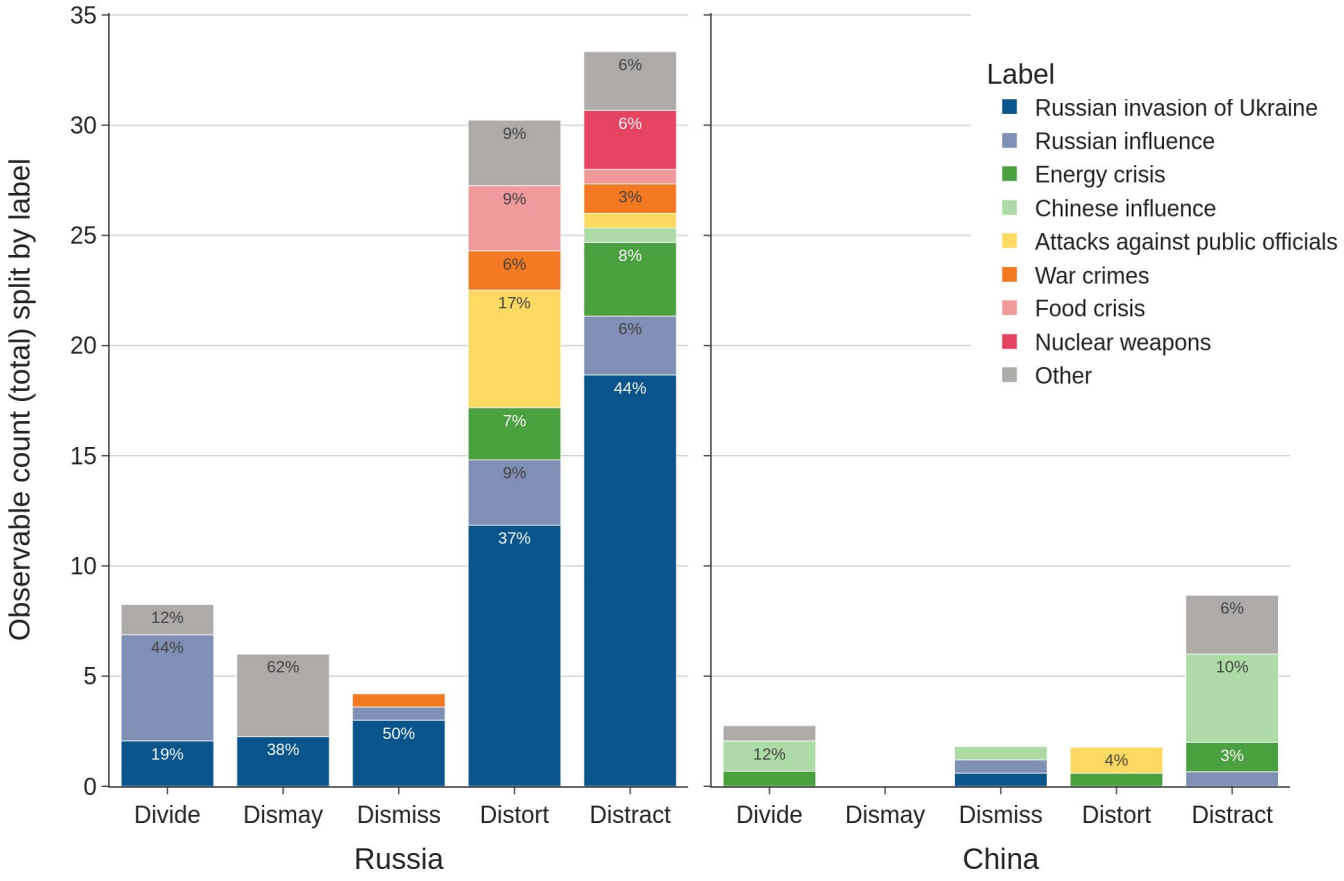


Figure 5 Total count of incidents per actor according to the presumed objective per topic

In the case of incidents carried out by channels linked to **Russia, 42% were intended to distract**. The large majority of incidents was used in the context of the Russian invasion of Ukraine, to turn attention to a different actor/narrative or to shift the blame (namely to Ukraine and the EU). Another **35% aimed to distort**, twist and frame narratives around the Russian invasion of Ukraine and to deliver attacks against the Ukrainian government and EU officials and institutions (such as the HR/VP). All incidents related to the energy crisis were also linked to these two objectives.

Russia used the Divide objective in incidents highlighting the West's alleged Russophobia or promoting Russian worldwide influence in order to create conflict and widen divisions within or between communities and groups. Top-targeted entities by these incidents were the government of Kosovo (in the context of the tensions with Serbia) and Poland.

In the case of **China, the majority (56%) of incidents intended to Distract**. Chinese incidents used the promotion of China as a reliable partner and as a world leader while degrading the West – especially highlighting how the US allegedly destabilises the EU. These statements were promoted in the context of other events in real life (such as the food or energy crisis) to shift attention to a different pro-Chinese narrative. The US and the EU were the top-targeted entities by Chinese distractive incidents.

BEHAVIOUR

Tactics, Techniques, and Procedures (TTPs)

Across the 100 incidents, 308 occurrences of TTPs were recorded, 72 of those were unique techniques. Most of the identified TTPs fall under the preparation phase with 67% of all identified TTPs (Figure 6). The rest of the detected TTPs belong to the execution phase (20%) and planning phase (13%).

When it comes to the most frequently used TTPs, threat actors paid special attention to the production and fabrication of content. **The development of image-based and video-based content were the two most recurrent techniques employed.** Moreover, the use of formal diplomatic channels to distribute content was the most used technique to deliver content to online audiences. In order to maximize the exposure of the operations, the amplification of the content happened through cross-posting across groups and platforms

Figure 6 All unique techniques and the number of times they were used in the incidents per phases

to propagate the content to new communities within the target audiences or to new target audiences.

Based on the analysis of individual occurrences, **certain TTPs occur more often together**. These combinations of TTPs belong to one aspect of the overall attack patterns used by threat actors. To be able to identify trends in the combination of TTPs, we looked at the most common combinations of two TTPs (see figure 7).

According to the 10 most common combinations of TTPs:

- Fabricated image and video-based contents were used to degrade the adversaries' image or ability to act and to discredit credible sources.
- Formal diplomatic channels were used to discredit credible sources; to deliver image- and text-based content; to distort facts by reframing the context of events; and to degrade adversaries.
  - In the case of Russia, a possible reason for the increased use of diplomatic accounts could be a consequence of Russian state-controlled channels with a formerly broad reach being sanctioned in the EU.
  - Fabricated image- and video-based contents were distributed across multiple platforms to maximise the exposure of the content.

Each FIMI Incident analysed in this report was tagged with at least one or more topical labels used to group incidents together based on themes. The taxonomy of the labels used during the analysis has been in constant development to reflect the main topics and themes featured in the observables composing each incident.

The labels most frequently used referred to (Figure 8):

- **"Russian invasion of Ukraine".** Covers any matter related to the war in Ukraine. In this context, threat actors relied on the fabrication of image-based content (30%) and video-based content (27%) to conduct FIMI operations. 28% of the labelled incidents were carried out by diplomatic accounts and in 13% of the incidents legitimate entities were impersonated in order to give legitimacy to the content. The main intention was to degrade Russian adversaries in the war (22%).
- **"Russian influence".** Covers incidents promoting Russian objectives linked to achieving and expanding its influence in specific regions in the world while degrading other countries and entities. These incidents used breaking news events or active crises, such as the car plates dispute between Kosovo and Serbia, to promote Russia's image and global

influence. Fabricated image- and video-based content are the most used TTPs (41%). Similarly to incidents under the label "Russian aggression of Ukraine", these topical incidents used formal diplomatic channels to address their messages with the objective to degrade adversaries.

- **"Attacks against public officials".** Used when governmental officials and politicians are targeted in an incident. Threat actors make use of formal diplomatic channels to attack public officials (67%). These type of attacks frequently aim to discredit credible sources (42%), degrade adversaries (33%) and develop text-based (25%) and image-based content (25%).

Other relevant labels used were:

- "Chinese influence", which similarly to 'Russian influence' is used for the promotion of China as a reliable partner and as a world leader while degrading the West;
- "Energy crisis". For incidents concerning discussions on energy prices and energy shortages;
- "Bioweapons" and "Nuclear weapons" used when incidents mentioned either weapon category;
- "War crimes" used for incidents mentioning war crimes;
- "Gender disinformation", used when an incident has components of gender-based attacks;

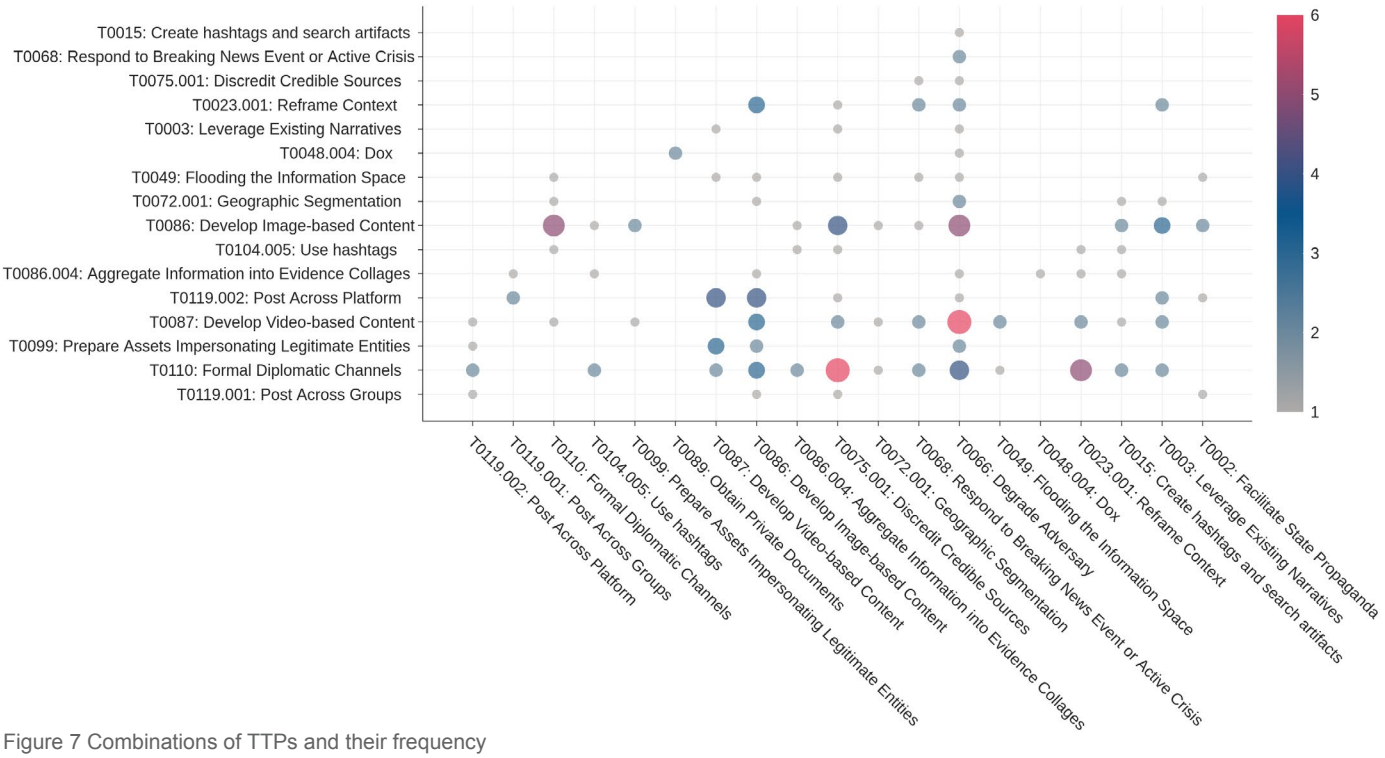


Figure 7 Combinations of TTPs and their frequency

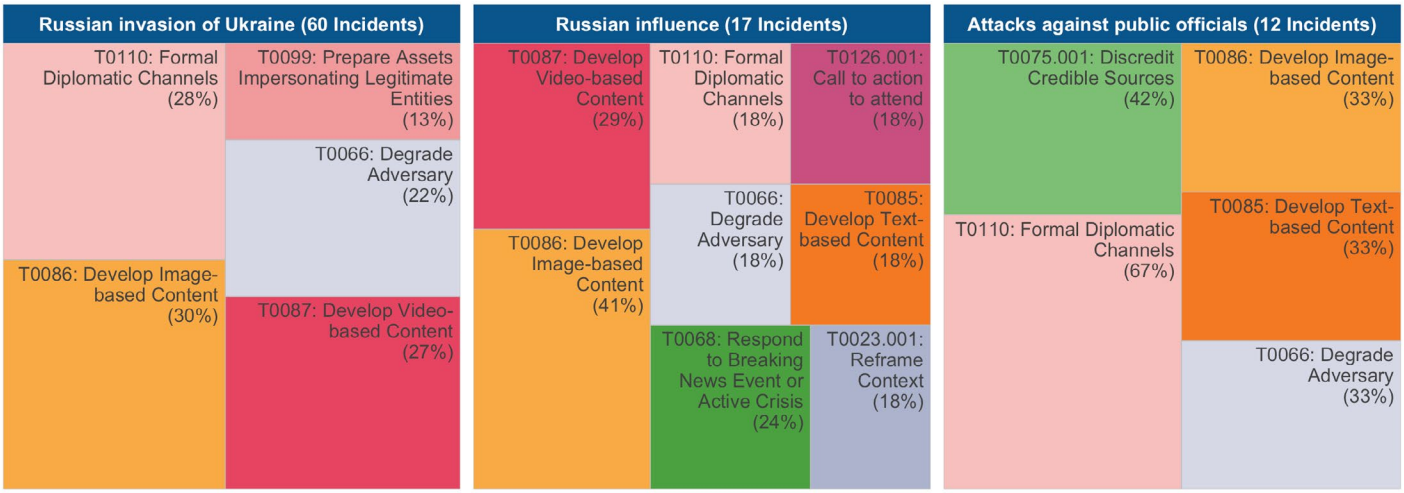


Figure 8 The most used TTPs per topical label

IMPERSONATION TECHNIQUES AND VICTIMS

A brief look into cases in which Russia impersonated legitimate, trusted entities illustrates that nobody is off limits from seeing their identity or brand misused. Threat actors use impersonation to add legitimacy to their messages and to reach and affect audiences familiar with and trusting the impersonated entities.

Six incidents used cases of impersonation. All of them related to the Russian invasion of Ukraine. **Media outlets were entities most frequently impersonated**. In four incidents, fake cover pages imitating the visual style of European satirical magazines, namely French *Charlie Hebdo*, German *Titanic* and Spanish *El Jueves*, were created to attack Ukraine and Ukrainian President Volodymyr Zelenskyy. Additionally, two videos imitated international media (*Aljazeera* and *Euronews*). The videos falsely claimed that Ukrainian football fans were detained in Doha because of Nazi behaviour during the World Cup, and that a German auction house was going to destroy Russian artworks. All while pretending the message originated from reputable media.

European institutions and politicians were the second most often impersonated entities (two incidents). An animated video listing the alleged disadvantages of Ukraine's accession to NATO, created using an AI-generated voice was presented as an official video by the European Security and Defence College. Moreover, a false account on Facebook used the name and personal information of the former chairman of the Lublin City Council (Poland) to publish a post on the missile blast in Przewodów.

According to preliminary investigations, a Russian attributed channel seemed to be the original publisher of the video impersonating Euronews. The rest of the cases were published by non-attributed channels in the Russian FIMI infosphere. However, the content was rapidly picked-up and amplified by channels attributed to Russian state structures, such as state-linked or state-controlled outlets.

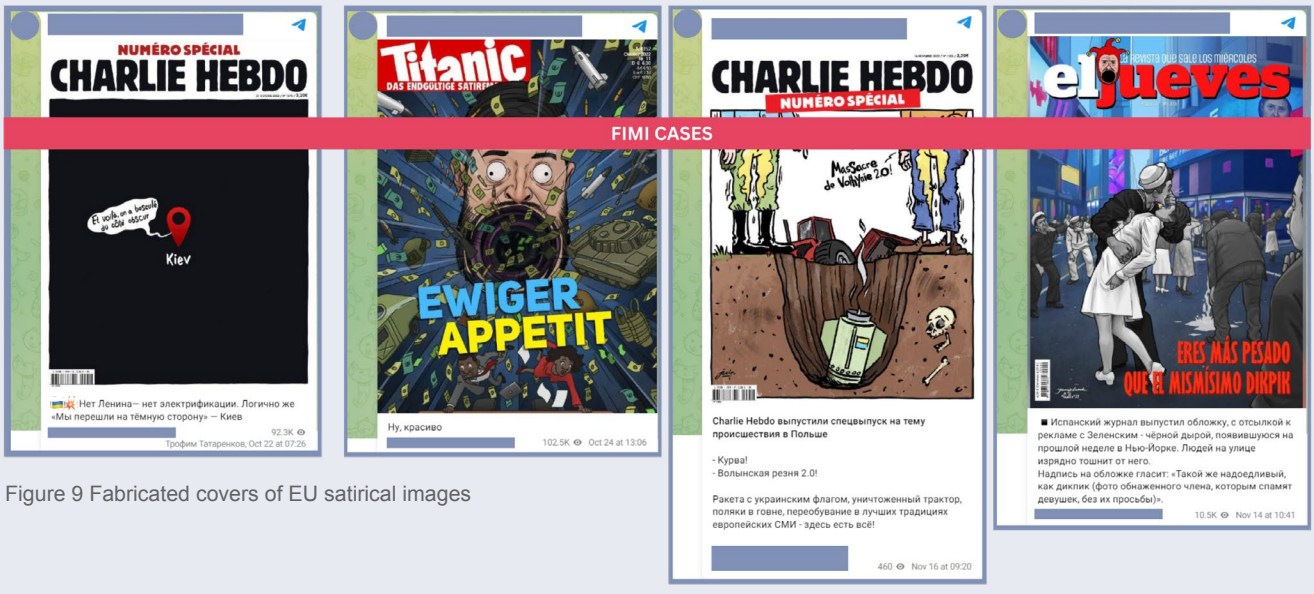


Figure 9 Fabricated covers of EU satirical images

CONTENT

The analysis of the content promoted in FIMI activities is a fundamental piece of the investigation. The content of the incident provides details on the narratives used, the socio-political context where the incident takes place and which content formats were preferred.

Timeline of Events

Since the 100 incidents analysed in this report were detected and documented between October and December 2022, the large majority of them, 866 observables (87% of the total number of observables) were published after the 1st of October. However, certain new incidents collected during this period were a **continuation of previous incidents or they recycled old content available online** (Figure 10). These incidents reused or referred to observables published earlier in 2022 or even earlier.

As an example of ongoing activities, since March 2022 a hacker group has been using a Telegram channel to promote their activities. Russian state-controlled outlets systematically amplified the content of this Telegram channel. On the 11th of October, the group posted new messages about successful cyberattacks against accounts allegedly "lying" about Russia's invasion of Ukraine (including Ukrainian news portals and institutions and companies from Latvia, Estonia, Lithuania, Slovakia, Poland, UK, US and Norway) (See figure 11).

Breaking news and events of regional and global significance are a prime targets for FIMI. These events draw media attention and are often surrounded by ambiguous and incomplete information, which makes it easier for threat actors to insert their messaging. Often, threat actors trigger FIMI incidents to influence the framing of such events or use them in the service of furthering their agenda.

Incidents can follow after an event took place, while in other cases, incidents were carried out to frame upcoming events. The events in our dataset include developments in Russia's invasion of Ukraine, high-level national and international summits, diplomatic visits and speeches by public officials, and the adoption of sanctions packages or legislation. Testing if certain events trigger a higher FIMI activity, we looked at events taking place during weeks with incidents featuring many observables:

10th Oct > 16th Oct: The week was dominated by incidents on the Russian invasion of Ukraine. The Kremlin FIMI ecosystem initiated a series of incidents alleging that NATO and the UK's intelligence services were involved in the **explosion of the Kerch Strait bridge in Crimea** on the 8th of October. The campaign would extend during the following weeks, including articles on proxy outlets and alleged leaked documentation. Moreover, the Russian FIMI ecosystem launched a series of coordinated publications on Telegram and Twitter sharing false narratives to sow panic hours after a Russian shelling in Kyiv on the 10th of October.

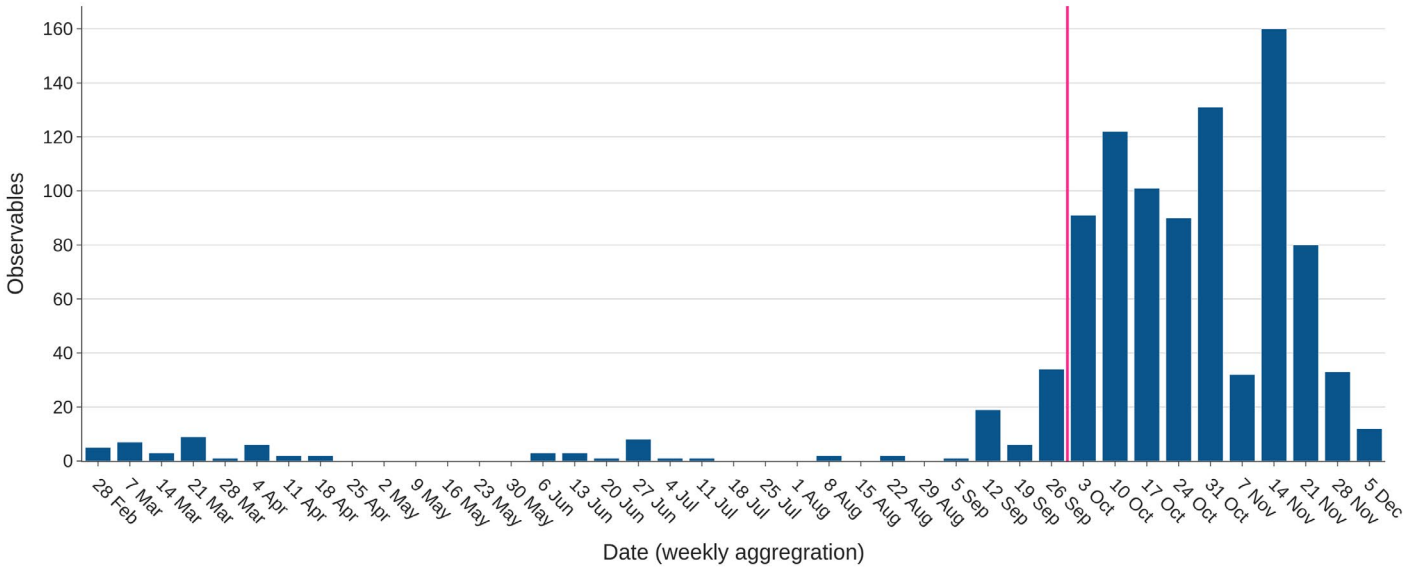


Figure 10 Weekly timeline of observables. On the timeline, observables that were published before the primary data collection (October, November and December) period are included

Figure 11 Messages published on Telegram by a hacker group incentivising cyberattacks against Western accounts allegedly "lying" about Russia's invasion of Ukraine through rewards in cryptocurrencies (above). The messages of the group were amplified by the Russian FIMI ecosystem (below).

That same week an alleged pre-bunking video of a civilian mass grave in Kupyansk claiming that it was Ukraine who had committed mass killings and another staged video showing the arrest of an alleged Ukrainian agent preparing a terrorist attack in Russia were promoted by the Russian FIMI ecosystem.

Threat actors also delivered incidents related to the 20th National Congress of the Chinese Communist Party as part of a campaign promoting positive views of China and the CCP globally.

31st Oct > 6th Nov: Eight incidents targeted Ukrainian officials and the Ukrainian Armed Forces. The Russian FIMI ecosystem produced videos and images implying that Ukrainian people do not support their President and Ukraine is supportive of Nazism. Moreover, Telegram was used by Russian FIMI actors to claim an alleged hack against NATO and Ukraine military systems.

The Russian FIMI ecosystem also launched new allegations that the UK and the US were involved in the Nord Stream pipeline explosions on the 26th of September by quoting fake correspondence between former UK Prime Minister Elizabeth Truss and the US Secretary of State Antony Blinken. This incident happened in parallel with the production of videos and cartoons about the rising energy prices in the EU and how the US is exploiting the EU economy.

14th Nov > 20th Nov: The 15th of November was a key date that triggered opportunistic incidents in the following days. On that day, **a missile exploded near Przewodów in Poland**. The Russian FIMI ecosystem amplified screenshots of a Facebook post published by a deleted account impersonating the former chairman of the Lublin City Council claiming that the missile blast was a provocation by Ukraine. Moreover, on the 15th of November the European Union Military Assistance Mission to Ukraine (EUMAM Ukraine) was launched; Russian diplomatic accounts

reacted by developing image-based content to degrade and dismiss the EU initiative and accusing the EU and NATO of conducting hybrid warfare.

Incidents trying to prove evidence of war crimes committed by Ukraine were highly prominent during the week. The campaign #StopKillingDonbass, launched in September 2022, tried to organise demonstrations in EU countries that week. The campaign uses graphic images and videos of corpses of minors and injured individuals holding a banner reading #StopKillingDonbass. Russian diplomatic accounts and channels who often interact with the Kremlin FIMI ecosystem were involved in the amplification of the hashtag across platforms falsely claiming that the Armed Forces of Ukraine and "neo-Nazi paramilitary units" commit atrocities against civilians, including children.

Moreover, the situation in Kosovo continued to be an event targeted by the Russian FIMI ecosystem with calls to action on Telegram to participate in barricades in North Kosovo. At the same time, Russia Today chief editor Margarita Simonyan announced the launch of the RT Balkan website and channels on social media.

Narratives

In order to document the main narratives present in the observables, a narrative taxonomy was developed based on the current dataset of incidents. Many of the narratives are linked to the Russian invasion of Ukraine, given that most of the incidents in the current dataset are related to the war.

- The most common narrative across the analysed incidents was the narrative '*the West is the aggressor towards Russia*', which includes messages that depict the West as being antagonistic towards Russia, pushing Ukraine to war, provoking and profiting off of the war, carrying out military mobilisation and being involved in actions that inflame tensions between Ukraine and Russia. This narrative was **observed in 17 incidents**.

- The narrative '*Ukraine is the aggressor towards Russia*' was observed in **15 incidents**. This narrative falsely portrays Ukraine as the one having provoked and wanting the war, committing atrocities, war crimes and genocide, and deploying or planning to deploy chemical/ nuclear attacks.

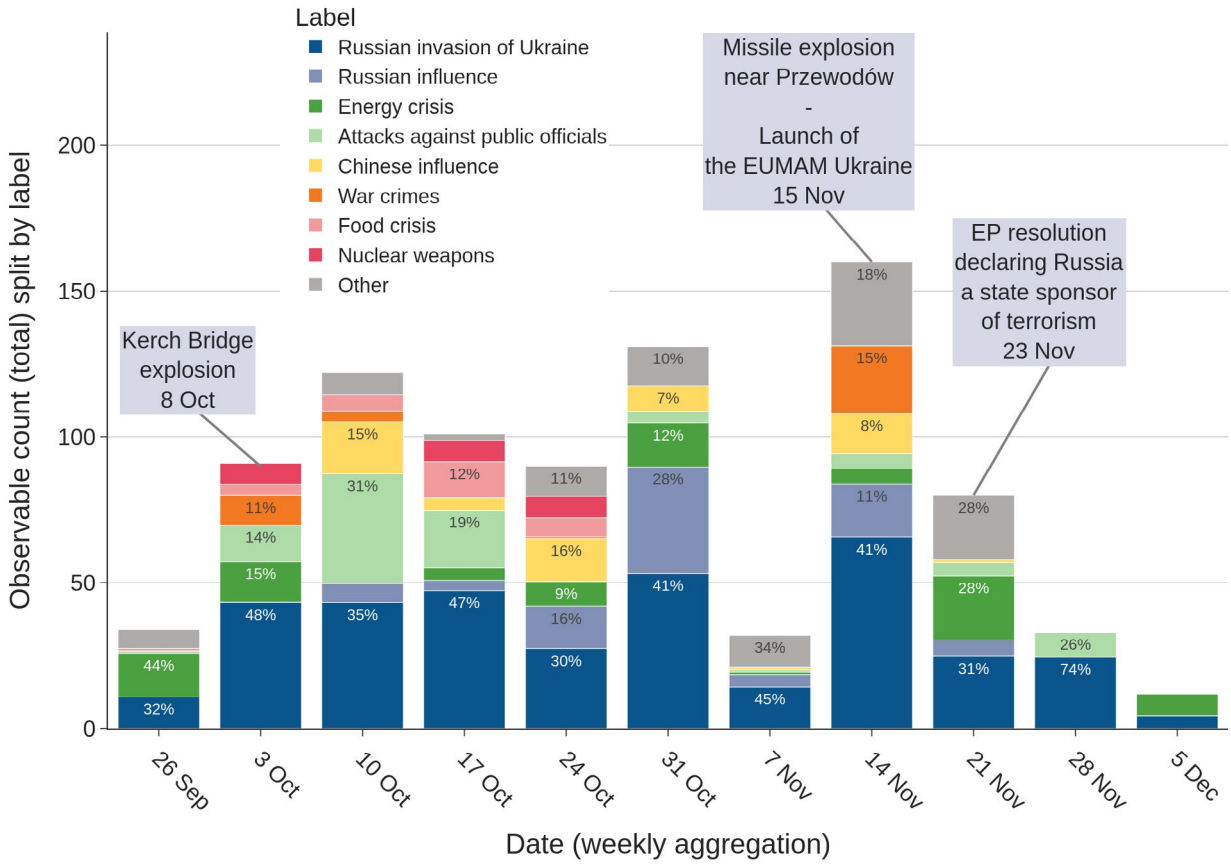


Figure 12 Weekly timeline of observables per label. Certain incidents were marked with more than one topical label. In these cases, the observables were also marked with multiple topical labels.

- The narrative '*the sanctions against Russia backfire*', which highlights the alleged negative consequences of the sanctions on Western and other countries, with a particular focus on the food and energy crisis as well as inflation, also appeared in **15 incidents**. It is worth noting that this narrative group also includes messages that allege that the current crises are caused by Western countries and their sanctions.

- The 4th most common narrative '*The West is hypocritical*', which includes all messages that falsely portray Western entities as abusing fundamental rights, carrying out disinformation campaigns, being corrupt, colonialist, russophobic or sinophobic, and exploiting others, was **observed 14 times**.

- The 5th most frequent narrative, '*Ukraine is a Nazi and terrorist state*', which features false claims that Ukraine is a Nazi and/or terrorist state or that they support such groups, appeared in **11 incidents**.

DEGREE

The degree dimension attempts to gauge and describe the way FIMI incidents travel through the information environment. This view on FIMI operations can reveal threat actor preferences with regards to targeted platforms and identify different roles of channels in a network as source, amplifier or link to other networks.

Composition of the Threat Actor Media Ecosystem

Russian and Chinese media ecosystems are composed by different networks of online and offline channels attributed to the official infrastructure of the government or ruling party. These online channels (websites, groups and profiles on social media) have been attributed according to high-confidence level indicators and can be classified in three groups:

1. **Official Communication Channels:** Channels officially used by a state and its representatives to deliver content. For example, official websites of a state or social media accounts of diplomatic services and embassies.

2. **State-Controlled Channels:** Media channels with an official affiliation to a state-actor. They are majority-owned by a state or ruling party, managed by government-appointed bodies and they follow an editorial line imposed by state authorities.[15]

3. **State-Linked Channels:** Channels with no transparent links nor an official affiliation to a state actor but their attribution has been confirmed by organisations with access to privileged backend data sources, such as digital platforms, intelligence and cyber security entities, or by governments or military services based on classified information.[16]

The channels operating in the threat-actors' ecosystems engage and interact with one another as well as other, so far unattributed channels in a broader digital infosphere. These unattributed channels are relevant as they are highly interlinked through technical, behavioural and contextual patterns.[17] Relevant, non-attributed channels in this infosphere contribute intentionally or accidentally to accomplish the objectives of FIMI activity. Unattributed channels that are found to regularly and significantly contribute to FIMI incidents' success can be identified more easily and prioritised for future research.

Altogether 616 digital channels played a key role in the original publication or amplification of the 100 FIMI incidents. Based on the categorisation system described above (Tab. 1), around 40% of the channels involved in FIMI incidents (245 channels) are attributed to the online ecosystems of Russia (207 channels) and China (38 channels). The remaining 60% (371 channels) that played a key behavioural role in the origin and early stages of amplification of the FIMI incidents were channels not attributed to Russian nor Chinese state structures.

Table 1 Count of channels involved in incidents by actor and group.

	Russian Ecosystem	Chinese Ecosystem	Total
Official Communication Channels	76	13	**89**
State-Controlled Channels	75	25	**100**
State-Linked Channels	56	0	**56**
Total Attributed	**(207)**	**(38)**	**(245)**
Total Non-Attributed		**371**	**616**

Threat Actors' Infosphere

Besides the three categories of attributed channels, the threat actor's ecosystem also relies on a wider infosphere of non-attributed channels and networks that engage regularly with the ecosystem in various degrees and roles.

Continuous analysis across multiple incidents can reveal their role and aid distinction as accidental or systemic and integral to the successful construction of FIMI supply chains. Relationships between channels are defined according to technical, behavioural and contextual indicators[18]. A systematic analysis of channels with significant involvement in incidents helps to determine the nature of connections between attributed and non-attributed channels.

The network graph below shows all channels involved in the 100 FIMI incidents. Each node represents a distinct channel. A connection between nodes is drawn when two channels were found to engage in the same incident. The graph is undirected and does not show which node influences another node just that they are acting together within the context of one incident.

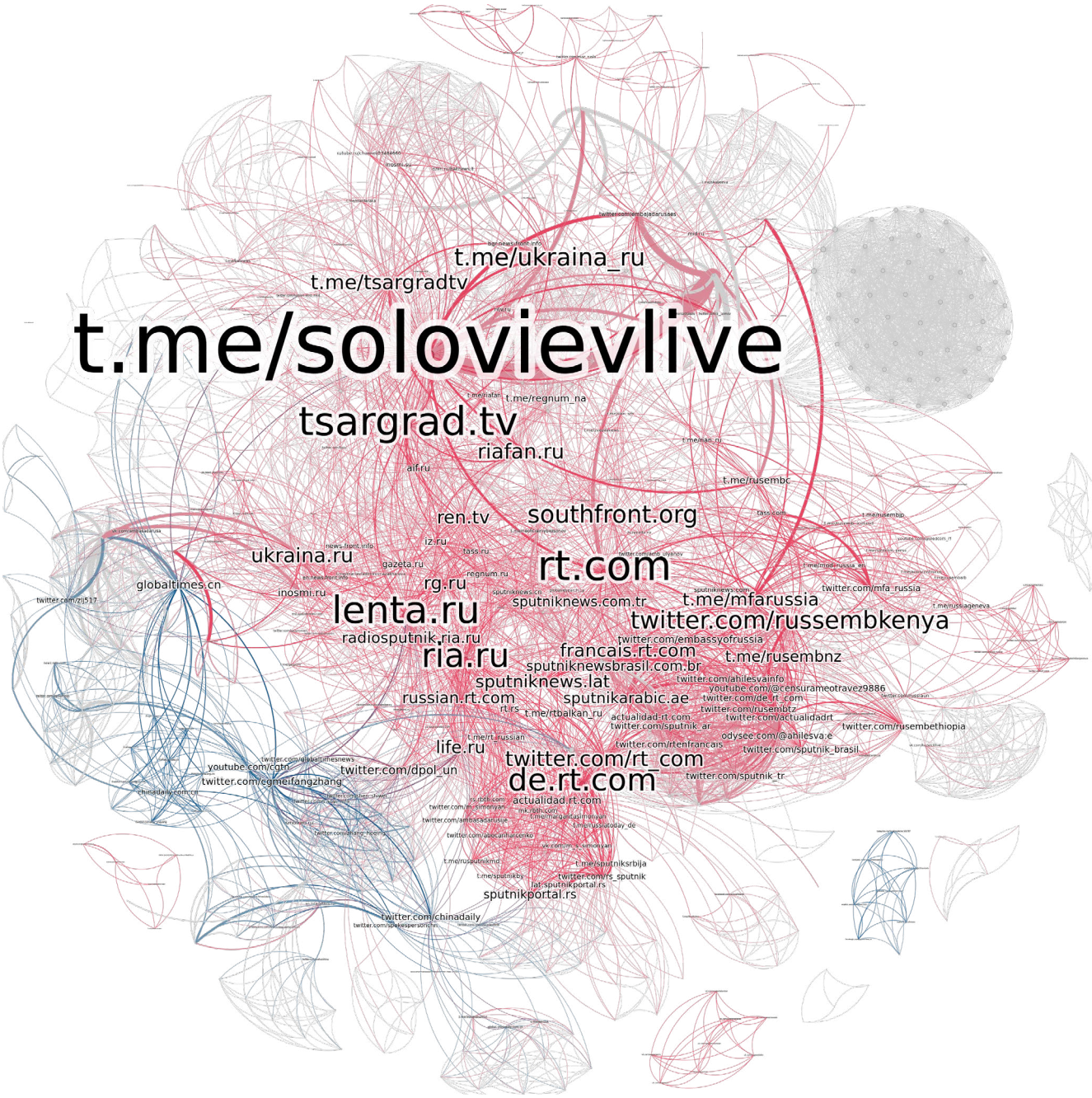


Figure 13 Network map representing the connections between all channels based on their involvement in the same incidents

Nodes are coloured according to the actor they represent: 85% of all coloured nodes are attributed to Russia and displayed in red, the 15% remaining coloured nodes in blue are channels attributed to China. Grey coloured nodes are not officially attributed to either actor and are not labelled. There are over 600 nodes shown in the graph with over 5700 connections between them. About 40% of all nodes have an attribution.

The nodes are sized according to how many connections they have to other nodes. The more connections a node has, the bigger it is and its label are displayed. Equally, connections between nodes (edges), are thicker the more often channels are found to act together across incidents. Thicker connections indicate that channels work more often together to engage in FIMI. Bigger nodes and labels indicate that channels are more often relied upon to engage in FIMI.

The graph provides many possible avenues for further analysis. What causes a large number of other channels to regularly interact particularly with the Telegram channel t.me/solovievlive? Which are nodes systematically bridging and connecting the Chinese and Russian infosphere that appear otherwise not very integrated? Who benefits from the densely coordinated subnetwork on the top right of the graph? What is its purpose and why does it appear to operate so differently from the rest of the network?

Graph insights can help us prioritise investigations and provide further indications for attribution based on behavioural patterns.

Tools: Distribution of Content

Threat actors select the most appropriate platforms to distribute and maximize the exposure of FIMI operations to their desired target audiences. Threat actors will evaluate platforms' usability and suitability, such as the exploitation potential of algorithms, content moderation practices and terms of service in order to select the most adequate infrastructure to deploy the arsenal of TTPs.

The **channel type classification** was developed using the current dataset of incidents using a simplified version of the "Select Channels and Affordances" DISARM tactic.

93% of the observables were published on social media platforms and websites. Social media platforms (63%) such as Telegram, Twitter and Facebook, are the most frequently used channel types to distribute incident content in our sample. 30% of the incidents used websites (news outlets, dedicated sites or websites of public bodies). The rest of the observables were detected in video sharing platforms (such as Youtube, Rutube, Douyin, Odysee, TikTok, Vimeo and Snapchat), discussion forums (Reddit and Quora), blogging and publishing platforms (WordPress, Medium, LiveJournal and Telegra.ph), content aggregators, photo sharing platforms (Instagram) and archiving platforms.

The ease with which content can be replicated via social media or networks of (inauthentic) websites is of particular relevance given our earlier finding that older material (observables) is frequently reused in future incidents.

Languages

The data collection includes observables in 30 languages (Figure 14), 16 of them EU official languages (BG, CZ, DE, DA, EL, EN, ES, FR, IT, LV, LT, NL, PL, PT, RO, SV). A big proportion of the observables were in Russian (38%) and in English (36%). In 23% of all observables, threat actors tried to reach different geographical audiences by making the content available in multiple languages. The most common combinations of languages are English and Russian, French and Russian, and German and Russian. In six observables of the data collection, the content was expressed in Russian and Chinese at the same time. This result reflects the 5 incidents where Chinese and Russian actors operate together in the same incident. After the original publication of the observables in English by Chinese channels, the Russian ecosystem adapted and translated the Chinese observables into Russian.

Russia used a larger variety of languages in their incidents than China in our dataset (Table 2). 44% of the observables targeted a Russian-speaking population. The second most used language by Russian actors was English in an attempt

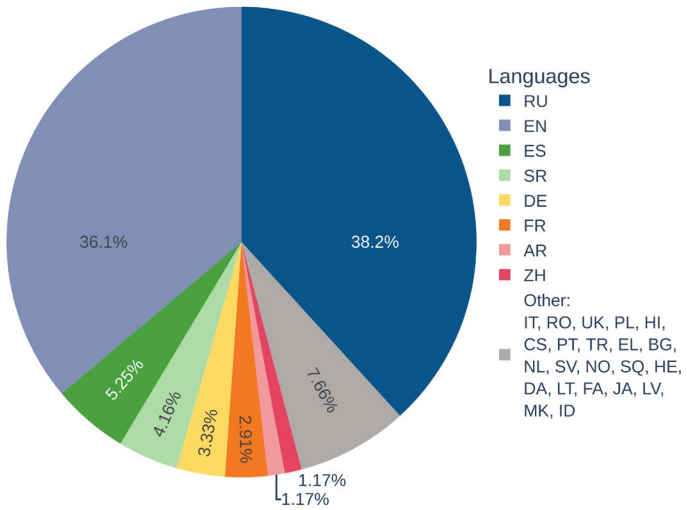


Figure 14 Distribution of the observables' languages

Table 2 Distribution of observables' languages per threat actor.

	Language	% of Observables		Language	% of Observables
Russia	RU	44	**China**	EN	71
	EN	29		RU	11
	ES	5		ES	5
	SR	5		ZH	3
	DE	4		DE	1

to reach audiences that are more global. Incidents in Spanish (5%) and Serbian (5%) tend to use one single language and they did not appear combined with Russian. China used English as a vehicular language (71%) instead of Chinese (3%). This indicator suggests that Chinese channels addressed global audiences instead of a Chinese speaking population overseas. 11% of the content from Chinese incidents was in Russian and 5% in Spanish.

Targets

For each incident, the targeted entity was also recorded. We distinguish between countries, individuals or organisations that an incident targets. In certain cases, no target entity could be identified, while in others, multiple targets were recorded[19]. **Altogether 77 unique entities were targeted 185 times. Among the targets were 6 countries, 23 individuals and 48 organisations.**

As described in the section dedicated to "Presumed objectives", threat actors' activities try to turn the attention to other actors, to accuse their enemies or to push back criticism. Therefore, the entities responsible for the conflict in Ukraine – according to Russian and Chinese actors – are the organisations most heavily targeted by Incidents.

Ukraine was the main, direct target of incidents 33 times in total (Figure 15). The EU was targeted 15 times (8%), HR/VP and the United States of America 11 times (6% each), while the Armed Forces of Ukraine were targeted 10 times (5%). We encoded countries as targets when representatives or organisations representing a country were targeted.

Other identified targets were international and intergovernmental organisations, namely NATO and the United Nations.

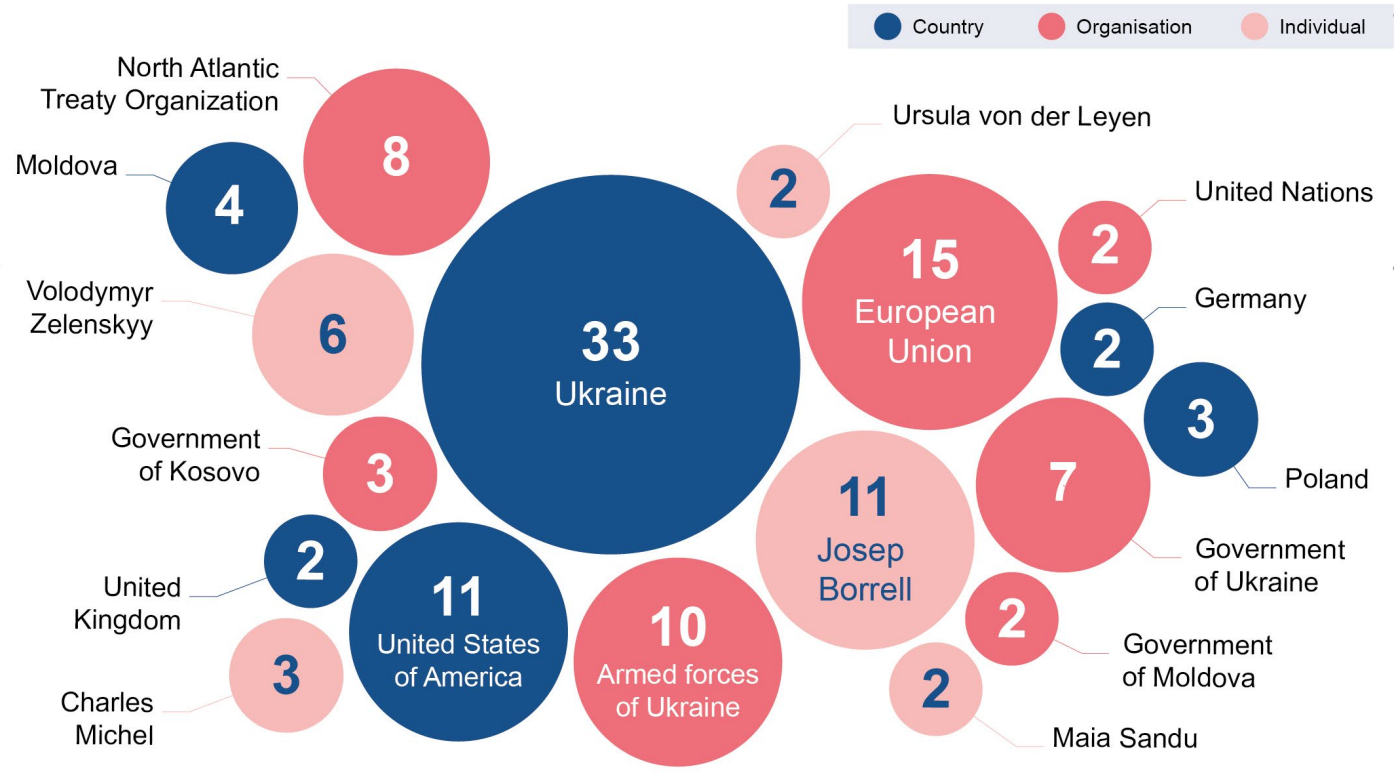


Figure 15 Top targeted entities and the number of times they were targeted

When it comes to individuals, leading EU figures such as the HRVP, President of the European Council Charles Michel and European Commission President Ursula von der Leyen, as well as Heads of States, such as President of Ukrainian Volodymyr Zelenskyy and President of Moldova Maia Sandu are among the most targeted.

EFFECT

The effect of an incident (or the impact or severity) can be measured and assessed according to different parameters such as the reach, the reach outside of in-groups, engagement, harm or behaviour-change caused offline etc. The full effect an incident can achieve will depend on its successful completion. Incidents with a high effect will not have caused their maximum damage in the early stages of an attack, where interventions will provide their biggest added-value. Depending on what FIMI defenders seek to protect, **reverse-engineering the attack patterns and chronology of past highly effective incidents can provide valuable indicators** as to which possible or unfolding incidents to focus their attention on to avoid or reduce the most harm.

One of the objectives of the methodology outlined in this report is to enable the results of the analysis to inform effective and appropriate countermeasures against FIMI across the available spectrum. This requires a systematic record and evaluation of countermeasures deployed under various circumstances. This data is still incomplete and requires information exchange between analysts and those deploying countermeasures. The Course of Action STIX object enables us to record and attach counters to incidents.

Course of Action

The Course of Action refers to actions taken by any entity in response to an incident, in order to counter the impact of it. Based on the current dataset of incidents, six categories of countermeasures were identified:

- **Statement of Refutal:** An involved entity issued a statement refuting the claims of the incident.
- **Debunking:** The claims of the Incident were debunked/ fact-checked.
- **Content Deleted:** Content of any type was taken down in response to the incident.
- **Content Confined:** Content of any type was limited in response to the incident.
- **Channel Limited or Suspended:** The channel of any of the observables was limited or suspended in response to the incident.
- **Other:** Any other counter measure that is not captured by the above taxonomy.

80% of the incidents did not trigger any type of response – according to our manual researches. However, 20 incidents received a communication response according to the previous categorisation. In some cases, more than one countermeasure was taken. Altogether, we identified 28 countermeasures taken in response to the incidents.

The most common countermeasure were statements of refutal, when an involved entity issued a statement refuting the claims of the incident, making up 50% of all courses of action. In 5 cases, the channel involved in the incident was limited or suspended, while in response to 4 incidents, the observables' content was confined. Debunking or fact-checking of the claims of the incident happened in 3 cases. The least common countermeasure was the deletion of content, as it only happened in response to one incident.

In the context of the Russian invasion of Ukraine, countermeasures for 18 incidents were recorded. In the majority of the cases, it was the targeted entities who responded to the incident publishing a counterargument or exposing the attackers when their accounts on social media were impersonated or compromised. The **entities that responded to incidents are media outlets** (German TV channel ZDF and Euronews), **governments and politicians** (Moldovan Ministry of Defence, President of Moldova Maia Sandu, Ukrainian President Zelenskyy's spokesperson, the Ukrainian Institute of Reproductive Medicine, Centre for Strategic Communication and Information Security of Ukraine and Ukrainian Ministry of Health, among others). **Third party organisations** (such as NGOs, media researchers and fact checkers) were the second type of responders while **platforms responded in two incidents by suspending accounts**.

Table 3 Distribution of the Course of Action types

Course of Action	%
Statement of Refutal	50
Channel Limited or Suspended	18
Content Confined	14
Debunking	11
Content Deleted	4
Other	4

4 A BEHAVIOUR-CENTRED PROBLEM DEFINITION: INTRODUCING THE NOTION OF FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI)

DEFINITION

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.

The analysis and overview over the 100 incidents represent a sample that was analysed with a specific focus on manipulative behaviour. This section discusses the conceptual perspective on the "disinformation" problem that underlies the **EEAS's approach to detecting, analysing, and disrupting** attempts by foreign actors to manipulate information environments and interfere in democratic processes. The EEAS has been leading efforts to more clearly define the actual threat in its complexity, going beyond the surface of content and understanding the behaviour of FIMI actors. This section introduces the notion of **Foreign Information Manipulation and Interference** (see definition box), which **overlaps with the notion of disinformation, but is at the same time narrower and broader**.

It is narrower in that it only refers to information manipulation by actors foreign to the EU and its member states, thus **not applying to domestic sources**. It is broader insofar as it **does not require the information spread by threat actors to be verifiably false or misleading**. The deciding factor for whether something can be considered FIMI is not false or misleading content, **but deceptive or manipulative behaviour**.

An instructive and intuitive example of FIMI is CIB on social media platforms, in which threat actors aim to portray a narrative to be more widely supported than it is by amplifying it through fake and deceptive social media accounts. The information spread by these networks does not need to be verifiably false or misleading to constitute a FIMI incident, which makes FIMI broader than the classical definition of disinformation.

Detaching the problem definition from the presence of verifiably false or misleading narratives serves to better capture the breadth of manipulative activity by foreign threat actors. At the same time, the behaviour-centred aspects of the FIMI definition are just a **formalisation of how many analysts in the defender community have approached the distinction between mis- and disinformation**, i.e. genuine belief in misleading or false information versus the self-serving intent of the threat actor.

Researchers have typically referenced deceptive or manipulative behaviour, for example in the form of spoofing well-known news outlets,[20] to distinguish between disinformation and misinformation cases. The FIMI definition highlights this research practice that **intentional manipulation of the information environment (disinformation), and the sharing of genuinely held but verifiably false or misleading beliefs (misinformation), are two different problems** requiring different conceptual and political responses in terms of effectiveness and appropriateness.

THE "KILL CHAIN" PERSPECTIVE ON FIMI: EXPANDING THE COUNTERMEASURES TOOLBOX

Accentuating the behavioural aspect of the problem is not only conceptually coherent with research practices in the FIMI analysis community, but also **enables us to expand our toolbox of countermeasures in addition to the focus on strategic communication as well as pre- and debunking of misleading or false narratives**.

An actor who wishes to manipulate the information environment needs to follow a series of steps (tactics) in order to conduct their attack. Each actor can choose from a range of different techniques per tactic to complete this step. For example, in order to create legitimacy for certain claims, some actors chose to compromise trusted, real accounts to spread their message while others chose to impersonate legitimate sources of information. These are two different techniques to achieve the same tactical objective of increasing the credibility of a claim. Once completed, threat actors would then move to the next steps of amplifying content via other techniques. The combination of all techniques in an attack constitutes the attack's procedure.

Understanding a threat actor's behaviour as a process ranging from planning, preparing, and executing to assessing is referred to as a "Kill Chain" approach to FIMI and disinformation.[21] So named because denying a threat actor the completion of one step in that process would "kill" the attack. This approach builds upon positive experience in cybersecurity, where the forensic analysis of threat actor behaviour throughout the entire timeline of their attempted attack has helped to better understand systemic vulnerabilities, and how to spot and close their exploitation to prevent the infiltration of and damage to computer systems.[22]

There are important differences between computer systems and the information environment, for example in terms of sociological complexity. However, given prior work like Graphika's "Secondary Infektion"[23], where a threat actor was found to reuse specific techniques and combinations thereof, many times and in different circumstances, such a "Kill Chain" approach to FIMI appears promising to expand our capabilities for detection, analysis and possibly attribution.

The Kill Chain approach broadens and structures our perspective on FIMI. We can ask what a threat actor was doing before they were able to deploy a message; where in the attack chain they are currently and what their next step(s) may be. Systematic collection of information across many incidents can inform which behaviour or combination of techniques is more likely.

Each step of the kill chain favours not only different approaches to detection and analysis but also response. An example from 2021 illustrates what early detection and response can look like to prevent a FIMI campaign from having impact: thanks to prior awareness raising efforts by the defender community on FIMI actors, strategies and targets, online influencers in 2021 were able to identify and call out preparatory steps of a FIMI campaign attacking the COVID-19 Pfizer vaccine. They were contacted by a shadowy marketing company asking them to present allegations against Pfizer as their own genuine opinion and took these requests for undisclosed influence public, likely preventing many from being exposed to the campaign[24]. However, even before the influencers had been contacted by the fake marketing company, a network of inauthentic news and lifestyle websites hosting the false allegations was created. The influencers were asked to reference these websites on their channels without disclosing that this was a paid-for request. These websites however remained undetected up until the time investigations into this FIMI campaign were further advanced. When FIMI content has been published, early detection and official rebuttals can deny a campaign its desired reach. Fact-checking and debunking are suitable responses when FIMI attacks have further matured along the kill chain and already reach or are likely to reach a wider audience.

THREAT ANALYSIS VS. DISRUPTIVE RESPONSES

For a Kill Chain perspective to be helpful in the systematic disruption of FIMI, it is necessary to consider two additional aspects. On the one hand, we need to **(1) objectively analyse the behaviour and TTPs threat actors use** in their efforts to manipulate the information environment. Doing so enables us to understand which vulnerabilities are most often exploited, and which ones lead to the most detrimental impact on the integrity of democratic processes and universal values. On the other hand, we need to **(2) systematically develop and measure disruptive responses**, investigate their efficiency in terms of closing vulnerabilities and disrupting FIMI logistics, and understand potential negative side effects of these responses.

For more optimal solutions, we propose to operationally separate but increase information sharing between Threat Analysis and Disruptive Response challenges in our approach to tackling FIMI.

As countering FIMI is about protecting the integrity of democratic processes and universal values, any response to FIMI needs to **be appropriate in relation to the seriousness of the threat. Responder challenges are explicitly normative in nature**, which needs to be acknowledged and treated as such. For example, the analysis side might help us to understand the centrality of online anonymity for a threat actor's success in manipulating the information environment, but responders will need to weigh whether challenging that central feature of the internet is proportionate to tackling the risk.

It is therefore not only important to assess the efficiency and desirability of responses to FIMI, but also to understand **which (political) actor is best placed to implement efficient responses** in different contexts. Based on the conceptual distinction between analysis and response, it is important to note that **this report focuses on analysis**. Insofar as the pilot study mentions responses, it is in a purely descriptive way relating what actors other than the EEAS have done to mitigate the impact of a FIMI incident at the time of analysis.

5 AN ANALYTICAL FRAMEWORK FOR FIMI THREAT ANALYSIS

Building on Camille François's ideas,[25] **James Pamment's ABCDE framework** proposes to differentiate FIMI incidents in terms of actors, behaviours, content, degree, and effect (see Table 1).[26] This framework forces analysts to ask comprehensive questions about threat actor activity and, in many ways, forms the basis and inspiration of the proposals discussed in this section. It is a **helpful mnemonic for both investigators and readers** to check whether an analysis covers every important aspect of a FIMI incident.

The ABCDE framework is helpful to start thinking about the essential elements of FIMI incidents. Enriched with **common taxonomies** for its ABCDE sub-categories and **guidelines to operationalise data collection, it guides research to fully understand one FIMI incident**. To derive general insights on FIMI, such a complete qualitative analysis can be repeated across multiple incidents to reveal cross-incident patterns by threat actors.

The analytical framework proposed in this section is the basis for how the EEAS currently collects **comparative data on threat actor behaviour** to enable insights into temporal, geographic, and cross-actor trends that could **help policymakers understand where and how to intervene**. The first element of the analytical framework is the formalisation of a strategic and self-reinforcing analytical workflow (see Fig.16). "Self-reinforcing" means that the more often the analytical workflow is applied, the better informed each research iteration will become.

Figure 16 Self-reinforcing workflow for strategically analysing incidents of Foreign Information Manipulation and Interference (FIMI).

The second sub-section is dedicated to the DISARM framework,[27] which is an independent, community-oriented, and open-source taxonomy of TTPs created by Credibility Coalition's MisinfoSec Working Group that "*map[ped] information security (infosec) principles onto misinformation.*"[28] – i.e., a promising proposal for operationalising the concept of 'behaviour' in the ABCDE framework. Finally, we propose an initial set of threat indicators inspired by cybersecurity's Structured Threat Information Expression (STIX™), a data format for standardising information on threat actor behaviour and infrastructure.

Table 4 The ABCDE framework for FIMI analysis according to James Pamment.

Actor	*What kinds of actors are involved? This question can help establish, for example, whether the case involves a foreign state actor.*
Behaviour	*What activities are exhibited? This inquiry can help establish, for instance, evidence of coordination and intent.*
Content	*What kinds of content are being created and distributed? This line of questioning can help establish, for example, whether the information being deployed is deceptive.*
Degree	*What is the distribution of the content? Which audiences were targeted and reached?*
Effect	*What is the overall impact of the case and whom does it affect? This question can help establish the actual harms and severity of the case.*

ANALYSIS CYCLE: ESTABLISHING A STRATEGIC AND SELF-REINFORCING WORKFLOW

The Analysis Cycle is a **meta-methodology to provide one core workflow that delivers both on the long-term objective of systematically analysing and disrupting FIMI and providing insights in the short-term for quick and timely reactions**.

In the **(1) Strategic Monitoring** phase, the ecosystem of known FIMI assets used by a threat actor to engage in manipulation is mapped. These assets can be overtly associated with a foreign actor, or have been attributed by the FIMI research community according to current best practices.[29] A good example of such a mapping is the infographic "Russia's Disinformation & Propaganda Ecosystem" depicted in Figure 17 (later also built upon by euvsdisinfo.eu).[30] Systematically monitoring the activity of these known FIMI channels allows us to understand patterns in their behavioural tactics, and spot potential new channels of that ecosystem, for example through suspicious amplification patterns of hitherto unknown outlets.

The **(2) Prioritisation & Triage** phase aims to filter the onslaught of activity by these FIMI channels to high priority and potentially harmful instances. Beyond ensuring that the data collection aligns with the definition of FIMI, we also prioritise incidents on issues that are of direct policy-relevance to and within the mandate of the EEAS. Systematically cooperating with other stakeholders in the FIMI analysis community that cover the respective priority actors and issues of their organisation completes the picture. This last point is why a shared analytical framework and methodology is so crucial for successfully disrupting FIMI globally.

Next, the **(3) Incident Analysis & Evidence Collection** phase focuses on an open-source analysis. This includes the connections between different channels of the ecosystem, for example in terms of how they amplify a specific piece of misleading content, where it was seeded, and what TTPs were used in the process of doing so. At this stage, analysts encode data on the incident according to the taxonomies outlined below. Since threat actors often delete traces of their activity once they achieve their objective, it is important to systematically archive evidence for future reference. In doing so, analytical operations need to be consistent with their organisation's commitments to comply with the General Data Protection Regulation (GDPR)[31] as well as with best practices for archiving evidence in a reliable and trustworthy way. For practical guidance, see the *Berkeley Protocol on Digital Open-Source Investigations*.[32]

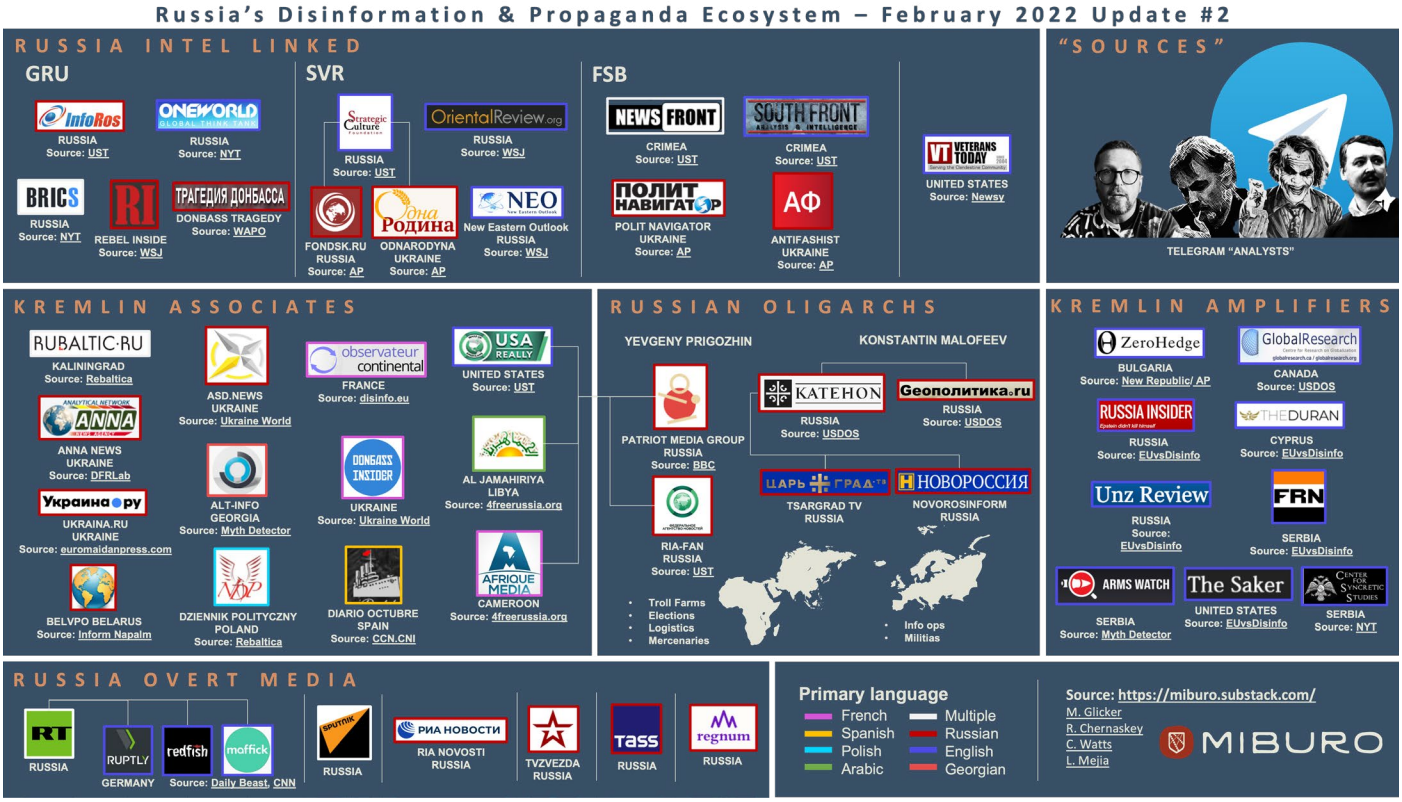


Figure 17 Mapping of known Russian FIMI channels including both overt and independently attributed covert operations according to Glicker, Chernaskey, Watts, and Mejia.

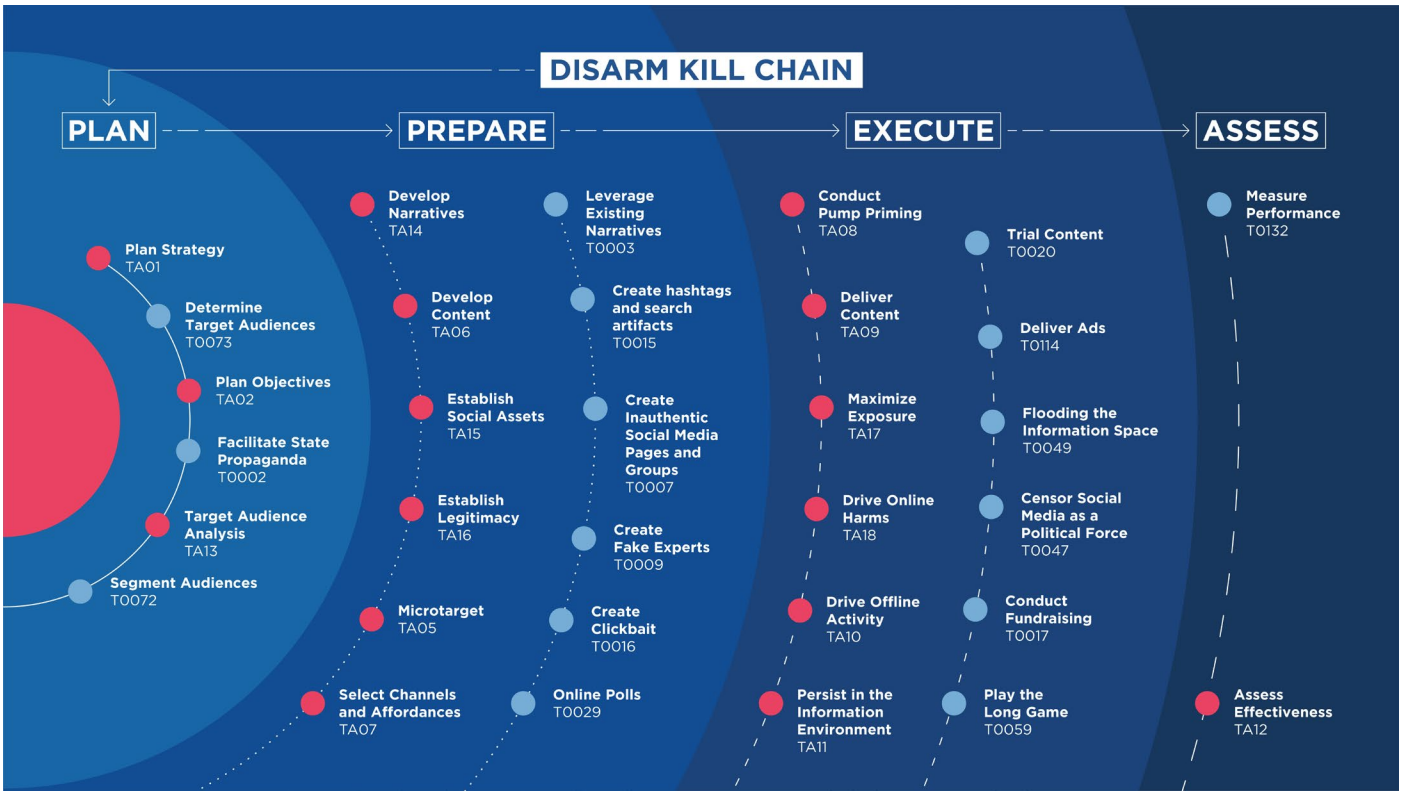


Figure 18 Visualisation of the DISARM framework's threat actor Kill Chain (Red Team). Red dots represent the overarching tactics (TA) at a given stage, blue dots show examples of techniques (T) used under a given tactic.

The **(4) Knowledge Pooling & Sharing** phase aims to maximise the short- and long-term utility of the analysis. In the short term, the analysis is shared with key stakeholders and partners that are in a position to immediately react to the incident, for example via strategic communication, public rebuttals, or, in the case of social media companies, by investigating whether the incident violates any of their terms of services. In the long-term, the standardised data on the FIMI incident is collected in a database that forms the basis for a comparative analysis of trends and patterns in threat actor activity over time. With more FIMI defenders maintaining their own but interoperable databases, knowledge pooling can be enhanced. This report's pilot study is a proof-of-concept of the benefits such an interoperable database offers.

Finally, **(5) Situational Awareness** is achieved by continuously optimising and reflecting on the previous steps, expanding the monitoring to newly attributed channels or new threat actors, and analysing patterns in the database resulting from this process. Adhering to this rigorous analytical approach builds up to a strategically important in-depth understanding of how, when, and where threat actors attempt to manipulate the information environment. Following this analysis cycle will yield actionable insights into weaknesses in threat actor behaviour, as well as societal vulnerabilities that need to be addressed.

DISARM FRAMEWORK: A COMMUNITY-DRIVEN TAXONOMY OF TTPS

At the heart of the Kill Chain perspective on FIMI is the systematic and granular data collection on TTPs used by threat actors to achieve their objective. We therefore need a taxonomy of FIMI TTPs that helps us to **operationalise the "B" in the ABCDE framework, which is *primus inter pares*** in our analytical framework. Any such taxonomy needs to be agile enough to adapt to new emerging TTPs, conceptually structured and specific enough to allow for the development targeted responses, as well as open-source to allow for maximum stakeholder inclusion and widespread adoption of a shared taxonomy.

Therefore, we strongly **advocate for a collaborative and community driven approach that enables each member of the FIMI defender community to contribute**. Such an approach would allow analytical teams from a wide range of stakeholders to weigh in with their specific experience and needs to optimise the shared taxonomy.

The **DISARM foundation's Kill Chain taxonomy** is currently the only framework that fulfils all of the above criteria, which is why it provides the **best-suited foundation for**

the community-led conversation on best practices this report encourages. While the DISARM foundation proposes an already elaborate taxonomy, it has been advocating for an inclusive and community-led development and testing of the framework illustrated in Figure 18.

Its disinformation Kill Chain, which is applicable to both domestic and foreign information manipulation, is **structured hierarchically by phases, tactics (TA), and techniques (T)**. Each phase – planning, preparing, executing, assessing – includes multiple tactics, which in turn contain multiple techniques. Figure 18 only shows illustrative examples of techniques as the framework contains more than a hundred to date. This initial proposal was developed based on a collection of open-source investigations into threat actor behaviour by civil society organisations, from which the framework extrapolated the most commonly used tactics and techniques.

As such, the framework represents the state-of-the-art of our understanding of FIMI operations, but **will continuously need to be updated** with new TTPs, **and optimised** in terms of the precision of the individual definitions and the reliability of measuring for the comparative study of trends. This report adds to prior proof-of-concept applications of the framework to empirical FIMI and generic disinformation cases.[33] Even though the framework is central to our analytical approach to FIMI, it is owned and managed by the DISARM foundation, which is in charge of handling suggestions for improvements by those using the framework.

The analysis of the behavioural components of an incident by means of identifying TTPs allows us to understand how a threat actor conducts their FIMI operations. The DISARM Framework divides the lifecycle of an incident in four phases. During the planning phase, threat actors envision and design the desired outcome of the operation. In the following Preparation stage, threat actors lay the foundations to execute the plan. In the execution phase of the incident, the activities are carried out via the previously established assets. In the last stage, the effect of the incident is assessed. In each stage of the process, threat actors can select between multiple TTPs to construct their attack.

If certain combinations of TTPs ("procedures") proved successful for an attacker and provided a good cost-benefit calculation, they are likely to reuse the same combinations, unless certain TTPs are rendered more costly or impossible. Reusing combinations of TTPs can aid attribution of attacks by establishing a threat actor's modus operandi or "behavioural fingerprint".

Detecting and disrupting TTPs early in the kill chain is one of the main objectives of systematically analysing behaviour across incidents in order to widen the available possibilities to counter an attack.

TOWARDS A STANDARDISED DATA FORMAT FOR THREAT INFORMATION SHARING

Commonly shared taxonomies are important to create a common language across a community to facilitate discussions while minimising potential misunderstandings. However, to effectively share insights – especially at scale – a common data format is also necessary. While far less often discussed, these technical standards are i.e. what makes the internet possible or that documents can be sent from one person's computer and edited by another person on another computer. **A common data format for sharing threat information is foundational for networked collaboration at scale.**

A basic requirement for such a data standard is for it to be able to represent all fundamental building blocks (or objects) of a threat and express how they are related to one another. It would also have to be flexible enough to remain useful while the threat keeps evolving, but stable enough to allow for the adaptation of processes and the building of tools on top of it. Lastly, it should follow the same principles of openness, community involvement and universality as commonly shared taxonomies to find wide adoption.

Given these parameter, the EEAS started encoding FIMI incidents in **the Structured Threat Information Expression (STIX™) format**[34]. STIX is "*a structured language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner*". It is an open-source framework owned and managed by the non-profit standards body OASIS Open. Even though it has been developed for cybersecurity incidents, STIX already covers many elements that are relevant in the FIMI context. Moreover, given a regular overlap between cybersecurity and FIMI incidents (e.g., in hack-and-leak operations),[35] aligning both domains' data standards would benefit cross-domain cooperation in both analysis and response to threat activity.

This report uses a **combination of existing STIX data objects and custom extensions needed for idiosyncratic FIMI threat indicators** not yet covered by the standard. Creating such custom extensions is intrinsic to the design of the STIX 2.1 version, and thus encouraged by its creators. However, to enable community wide adoption among the

Table 4 The ABCDE framework for FIMI analysis according to James Pamment.

STIX Object	*Description*
Incident	*Holds basic information about an incident (name, description, start date, objective etc.)*
Observable	*A url or file that has been observed in an incident.*
Channels (extension)	*Any online or offline communication channel (a website, social media profile or page, TV station etc.). Channels publish observables.*
Identity	*Individuals, organisations or locations including countries. Usually encoding the targets of incidents.*
Threat Actor	*Holds information about a threat actor*
Event (extension)	*Describes a real life event like an election, show, anniversary etc. to provide context in which incidents can take place.*
Vulnerability	*Describes a vulnerability that was exploited to make an incident work.*
Language (extension)	*Which language(s) was (were) used in an incident*
Attack Pattern	*Describes manipulative techniques (TTP) used to conduct an attack*
Course of Action	*Describes countermeasures to incidents.*
Narrative (extension)	*Describes narratives used in incidents. Narratives can be nested and be represented as meta- and sub-narratives.*

FIMI defenders, a consensus needs to be found whether to use STIX at all, which existing STIX objects to use, which to develop and how to use them. We hope this report provides a worthwhile starting point for that conversation.

The EEAS currently works with the STIX objects described above. Each STIX object has various properties like name, description, type, and date etc. to add information. STIX objects can be connected via relationships to express connections similarly to normal language, for example: the STIX object "*Threat Actor*" has the relationship "*targets*" to the STIX object "*Location*".

The advantage of decomposing FIMI incidents into these fundamental building blocks is that even partial information can add to increase situational awareness. FIMI defenders could for example just flag a new narrative that was spotted, or a new technique. It also enables specialisation in the FIMI defender community where analysts can focus on just monitoring and maintaining a continuously updated list of narratives or develop new capabilities to spot highly relevant TTPs.

CONCLUSION

The experience gathered by the EEAS in analysis and sharing information on FIMI since 2015 fed into this first report on Foreign Information Manipulation and Interference (FIMI). During this time, the defender community has achieved considerable progress and has continued to grow. With this evolution, that is encouraging in light of the ever evolving threat, comes the question of how all of this knowledge and insight can be brought together in an efficient and sustainable manner, complementing the existing practice of sharing reports on specific aspects of the threat. The EEAS in this report is proposing an approach which can enable the FIMI defender community to build on good case practices developed in- and outside the community to collectively achieve a more comprehensive situational awareness and inform appropriate countermeasures to the FIMI threat.

The report described and applied a methodology to reliably identify, analyse and share information on FIMI incidents. It outlined, based on a sample of 100 FIMI incidents, how building on shared taxonomies and standards can enable FIMI defenders to derive larger trends and patterns from their individual and collective findings to help inform appropriate countermeasures in the short to the long term.

In line with the EEAS' priority to work in a whole-of-society approach on tackling FIMI, the report strongly advocates for a collaborative and community driven approach that enables each member of the FIMI defender community to contribute with their unique skills, insights and perspectives.

Community-driven, shared taxonomies and standards like DISARM for FIMI TTPs or STIX for threat information storage and exchange are available and will facilitate deeper analysis, discussion as well as collective learning and action. Building on established open standards enables the usage and best case practice development and exchange of open source tools like MISP or OpenCTI and will pave the way for further innovation in the field. This also ensures an approach that is independent of the size or financial situation of an organisation, which makes a broad adoption also by think tanks, fact-checking organisations or NGOs possible.

Obviously, the EU deploys also other important instruments and tools to address FIMI. Among those are the use of restrictive measures, including those imposed against Russia in response to the unprovoked and unjustified invasion of Ukraine on 24 February 2022. The analysis of FIMI actors carried out by the EEAS has informed many measures taken so far.

Many possible avenues for further research have been identified in this report. For continuous and in-depth coverage, follow euvsdisinfo.eu.

RECOMMENDATIONS

1. A common analytical framework to facilitate multi-stakeholder cooperation requires consensus for wide adoption.
   a. Build on and enrich existing good-case practices, experiences and standards like STIX and DISARM where possible. Avoid the creation of parallel frameworks which would hinder interoperability.
   b. Favour widest possible adoption by endorsing and supporting open-source tools and standards that are community driven and informed by active usage of FIMI analysts.
   c. Prioritise interoperability of frameworks and standards to foster experimentation and innovation.

2. We suggest that the FIMI community convenes to agree upon a shared FIMI extension of STIX in the near future.
   a. In this regard, the creation of an Information Sharing and Analysis Center (ISAC) on FIMI can focus such discussions.
   b. Continuous interoperability of FIMI standards with other communities, like cybersecurity, should be ensured to realise the full potential of information sharing across sectors where appropriate.

3. Members of the FIMI defender community with the relevant means should engage in supporting community-driven initiatives that
   a. develop and maintain common standards and taxonomies for the benefit of the community
   b. engage in capacity building within the community by means of trainings, documentation etc.

4. For the wider community to increase the long-term impact of their insights by
   a. encoding and (re-) sharing research via interoperable data standards
   b. signalling findings and use cases not represented in commonly shared standards and taxonomies to the respective maintainers of these frameworks for the benefit of the community.

REFERENCES

1 European External Action Service (EEAS). October 2021. "Tackling Disinformation, Foreign Information Manipulation and Interference. Stratcom Activity Report." https://www.eeas.europa.eu/eeas/2021-stratcom-activity-report-strategic-communication-task-forces-and-information-analysis_en (all URLs were accessed on 24 January 2023)

2 European Commission. 2018. "Tackling online disinformation: A European Approach. COM(2018) 236 Final." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

3 European Commission. 2018. "Tackling online disinformation" (webpage) https://digital-strategy.ec.europa.eu/en/policies/online-disinformation

4 EEAS. 2022. "A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security." https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

5 DISARM Foundation. "DISARM Framework." created by SJ Terp and Dr. Pablo Breuer. https://www.disarm.foundation/framework

6 Hybrid CoE. 2022. "Hybrid CoE Research Report 7: Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM' " https://www.hybridcoe.fi/publications/hybrid-coe-research-report-7-foreign-information-manipulation-and-interference-defence-standards-test-for-rapid-adoption-of-the-common-language-and-framework-disarm/

7 Structured Threat Information Expression (STIX™). https://oasis-open.github.io/cti-documentation/stix/intro

8 EEAS Strategic Communication, Task Forces and Information Analysis (SG.STRAT.2); henceforward referred to as EEAS

9 European Commission. 2020. A European Democracy Action Plan. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en

10 EEAS. 2022. "A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security." https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

11 Jackson, Dean. 5 December 2022. "Influence Operations Researchers Want Guidance on Best Practice, But What Does That Mean?" Partnership for Countering Influence Operations, Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/12/05/influence-operations-researchers-want-guidance-on-best-practice-but-what-does-that-mean-pub-88517

12 https://euvsdisinfo.eu/

13 EEAS Special reports. https://euvsdisinfo.eu/category/blog/eeas-special-reports/

14 – Ben Nimmo, Central European Policy Institute. 19 May 2015. "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It." Blog Post on stopfake.org. https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/
– Cogsec Collab. 2019. "The 5D's (Dismiss, Distort, Distract, Dismay, Divide)." ADTAC Disinformation Inventory. https://inventory.adt.ac/wiki/The_5D's_(dismiss,_distort,_distract,_dismay,_divide)

15 Dragomir, Marius and Astrid Söderström. 2021. "The State of State Media: A Global Analysis of the Editorial Independence of State Media and an Introduction of a New State Media Typology." CEU Democracy Institute, Center for Media, Data and Society. https://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/2091/thestateofstatemedia.pdf

16 Pamment, James and Victoria Smith. 19 July 2022. "Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online." Report by NATO Strategic Communications Centre of Excellence and the European Centre of Excellence for Countering Hybrid Threats. https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244

17 Idem.

18 Pamment, James and Victoria Smith. 19 July 2022. "Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online." Report by NATO Strategic Communications Centre of Excellence and the European Centre of Excellence for Countering Hybrid Threats. https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244

19 It is worth noting that when the target of the attack was a head of state, governmental institution or other entities representing the state, the country of that entity was also added as a target.

20 EU DisinfoLab. 27 September 2022. "Doppelganger: Media clones serving Russian propaganda." https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf

21 – Schneier, Bruce. 24 April 2019. "Toward an Information Operations Kill Chain." Lawfare Blog. https://www.lawfareblog.com/toward-information-operations-kill-chain
– Bergh, A. 2020. "Understanding Influence Operations in Social Media: A Cyber Kill Chain Approach." Journal of Information Warfare, Vol. 19, No. 4, pp. 110-131. https://www.jstor.org/stable/27033648
– Nimmo, Ben and Eric Hutchins (Meta). 10 November 2022. Presentation on Overarching Online Operations Kill Chain. Cyberwarcon Conference. https://www.csoonline.com/article/3680149/meta-s-new-kill-chain-model-tackles-online-threats.html

22 Hutchins, Eric, Michael Cloppert, and Rohan Amin. April 2014. "Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." White Paper, Lockheed Martin. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

23 Graphika. „Secondary Infektion" 2020. https://secondaryinfektion.org/

24 RFERL, "Exclusive: Meet The Murky Russian Network Behind An Anti-Pfizer Disinformation Drive In Europe" 2021. https://www.rferl.org/a/russia-pfizer-covid-disinformation-serebryanskaya-murky-vaccine-influencers/31277170.html

25 François, Camille. 20 September 2019. "Actors, Behaviors, Content: A Disinformation ABC. Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses." Working Paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression.

26 Pamment, James. September 2020. "The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework." Working Paper of the Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Pamment_-_Crafting_Disinformation_1.pdf

27 DISARM Foundation. "DISARM Framework." created by SJ Terp and Dr. Pablo Breuer. https://www.disarm.foundation/framework

28 Credibility Coalition: Misinfosec Working Group. 2019. https://github.com/cogsec-collaborative/AMITT/blob/main/archived_version_of_AMITT/AMITT_HISTORY/2019-08-27_MisinfosecWG-2019-1.pdf

29 Pamment, James and Victoria Smith. 19 July 2022. "Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online." Report by NATO Strategic Communications Centre of Excellence and the European Centre of Excellence for Countering Hybrid Threats. https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244

30 Glicker, Max and Clint Watts. 25 February 2022. "Russia's Propaganda & Disinformation Ecosystem – 2022 Update & New Disclosures." https://miburo.substack.com/p/russias-propaganda-and-disinformation See also: US Department of State, Global Engagement Centre (GEC). August 2020. "GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem." https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

31 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

32 Human Rights Center (UC Berkeley School of Law) and UN Human Rights Office. 2022. "Berkeley Protocol on Digital Open Source Investigations. A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law." https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf

33 – Newman, Hadley. November 2022. "Foreign Information Manipulation and Interference Defence Standards: Test for Rapid Adoption of the Common Language and Framework 'DISARM'." Hybrid Centre of Excellence for Countering Hybrid Threats in collaboration with the NATO Strategic Communications Centre of Excellence. https://www.hybridcoe.fi/publications/hybrid-coe-research-report-7-foreign-information-manipulation-and-interference-defence-standards-test-for-rapid-adoption-of-the-common-language-and-framework-disarm/ – M-82 Project. 6 November 2022. "Disarm, une matrice pour décrire les campagne d'influence." https://www.m82-project.com/post/disarm-une-matrice-pour-d%C3%A9crire-les-campagnes-d-influence – Max Lesser, Hallie J. Stern and Sara-Jayne Terp. (DISARM Foundation). 9 November 2022. "Countering Russian Misinformation, Disinformation, Malinformation and Influence Campaigns in Italy Surrounding the Russian Invasion of Ukraine." Paper presented at the International Forum on Digital and Democracy (IFDaD). https://www.youtube.com/watch?v=jyGLwJ5RBS4

34 About STIX. https://stixproject.github.io/about/

35 ENISA and EEAS. December 2022. "Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape." https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape


European Union
EXTERNAL ACTION