EU CyberNet

Cybersecurity – information sharing and cooperation networks – and fighting disinformation – a bottom-up approach to reclaim safety in cyberspace

- Amit Ashkenazi

EU CyberNet Expert Series
No 1
2025

about

Amit Ashkenazi

Amit Ashkenazi is a law and technology expert, advising public and private organisations on legal, policy and compliance aspects of cybersecurity (including during cyber incidents), artificial intelligence, data protection, cloud use and ICT procurement.

Amit has been a legal advisor to the Israeli National Cyber Directorate (INCD) at the Prime Minister's Office from 2014 to 2022.

Before INCD, Amit was the Head of the Legal Department in the Israeli Privacy Protection Authority.

Since 2022, Amit has served as a consultant and academic and worked for the CT TECH project and has been a member of the OECD expert group on artificial intelligence and the expert group on privacy.

Since November 2023, Amit is part of the EU CyberNet Expert Pool.

summary

Cybersecurity professionals can play a key role in combating disinformation by targeting technical dissemination rather than moderating content. Using frameworks like MITRE ATT&CK and DISARM, they can detect and share information about disinformation 'kill chains', thus disrupting malicious spread of disinformation. EU policies, such as the Digital Services Act, support technical monitoring and information sharing. Recent cases, like foreign interference in Romanian elections, highlight the effectiveness of this approach. By focusing on transparency and preventing manipulation, cybersecurity experts can help protect the integrity of digital platforms while preserving free speech.

The purpose of this short blog article is to draw attention to the role of cybersecurity professionals and cybersecurity tradecraft in fighting *disinformation campaigns*. *Disinformation campaigns* mean *coordinated efforts* to spread *"false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm". [1]* Such campaigns have been integrated more and more in hostile cyber operations. [2] At the same time, taking action against disinformation campaigns is burdened by claims that such action means intervention in freedom of speech online. These claims, present since the early days of the Internet have come back to central stage, backed by strong political narratives. These claims have led to major changes in *content moderation* in the largest social media platforms.

Indeed, the battle against disinformation is challenging due to the sensitivity of any government institution interfering in content production and distribution. The well-founded concern is that *the medicine is worse than the cure* because it enables intervention in the *marketplace of ideas*. The basic wisdom is that the common cure is not less but more speech to enrich the *marketplace of ideas* and not stifle one sort of content. [3] But what if the *marketplace of ideas* itself, and in the internet context – *content sharing platforms*, is being misused or manipulated?

Once again, the purpose of this short article is to draw attention to the important role cybersecurity professionals have in developing *a potential middle ground for combatting disinformation*. This middle ground focuses on the *content dissemination process*, thus reducing the need to make decisions about the content itself. It aims to protect the *infrastructure of the marketplace of ideas* by identifying and mitigating *technical misuse* of the content sharing platforms and content distribution mechanisms. This approach is focused on dealing with the disinformation *kill chain*, the chain of actions a malicious and manipulative actor takes as part of its disinformation campaigns. Thus, it shifts attention and mitigation from looking at content (especially content that is not illegal *per se*) to the activity of malicious actors and to manipulative techniques of context distribution and specifically *technical indicators* of such behaviour.

As it will be described, bottom-up cybersecurity community activity and cooperation focusing on the *content dissemination process* and *sharing actionable information* related to malicious content distribution can curb the spread of disinformation and also bridge some of the emerging gaps in global policy and governance approaches. Such bottom-up approaches are also already complemented by top-down policy measures adopted in the EU that provide incentives that strengthen such efforts. [4]

The cybersecurity 'kill chain' and taxonomies for information sharing

The departing point for the discussion is the (now standard) cybersecurity imperative of sharing *actionable information* about attacker's *tools, techniques and procedures*. Numerous events have demonstrated that while each organisation (hopefully) monitors its own digital presence and manages its cybersecurity posture, it does not see what is happening in other organisations, which are also targeted by the same malicious actor. Sharing information across organisations enables a comprehensive view of the threat landscape and improves resilience and mitigation.

To operationalise this imperative, cybersecurity professionals require standard taxonomies and mechanisms of observing, analysing and disseminating information about attacker's tools, techniques and

procedures. Such standard taxonomies are essential for organising and communicating information in a clear and effective manner.

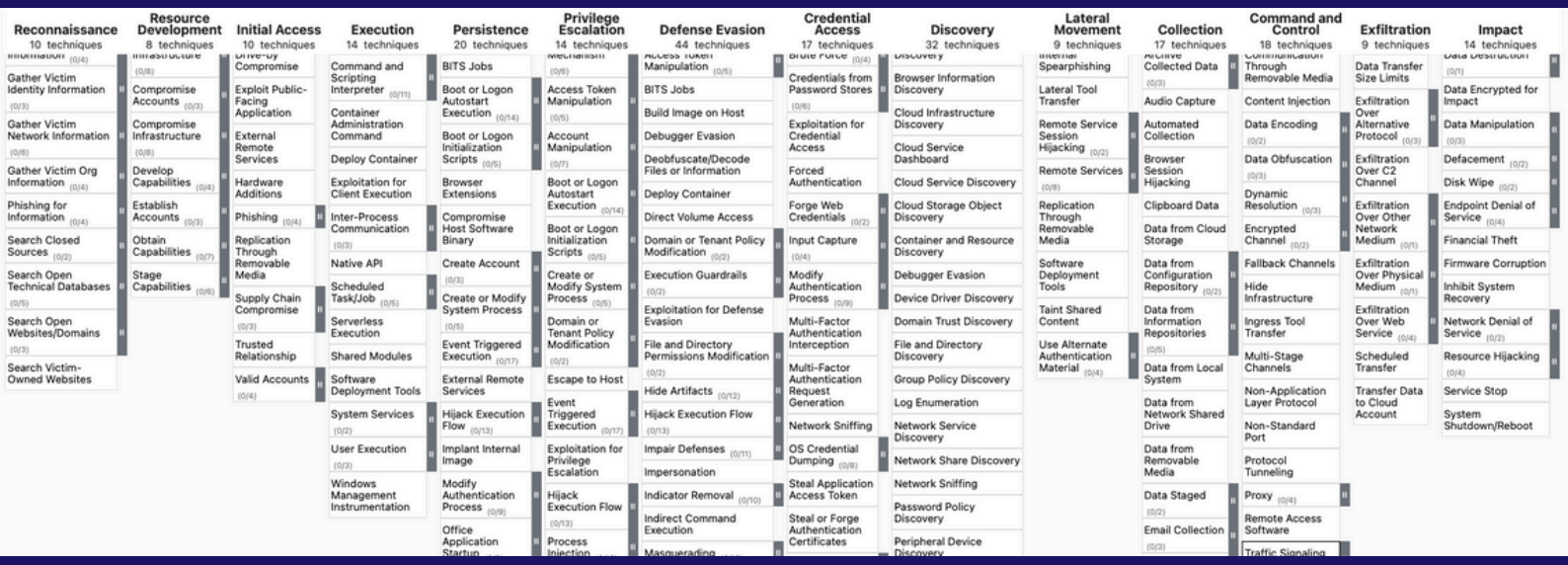
> *Cybersecurity teams can use MITRE ATT&CK for threat detection, threat hunting or penetration testing, by understanding how attackers might try to compromise their systems. Such understanding enables developing better detection rules, proactively search for malicious activity within their networks or penetration testing that simulates real-world attacks and identify vulnerabilities.*

MITRE ATT@CK Framework

The MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT@CK) Framework [5] provides such a taxonomy. It describes in detail the *cyber kill chain*, the chain of activities taken by a malicious actor as part of a cyber-attack. ATT&CK provides a common language for sharing information about adversary tactics and techniques. ATT&CK is organised into matrices that categorise adversary tactics (the *phases* of an attack) and techniques (the *how*). There are different matrices for different environments, such as Enterprise, Mobile and Industrial Control Systems (ICS). Thus, it provides a standardised framework for describing malicious activity and communicating about it in each phase of a cyber operation.

Organising and sharing this information supports cybersecurity operations at different phases of the cybersecurity lifecycle. Organisations can use ATT&CK to evaluate their current security posture and identify areas for improvement. Security teams can use ATT&CK for *threat detection, threat hunting or penetration testing* to understand how attackers might try to compromise their systems. Such understanding enables developing *better detection rules, proactively search for malicious activity* within their networks or penetration testing that *simulates real-world attacks and identify vulnerabilities*. During *incident response*, ATT&CK can help incident responders understand what an attacker might have done during a breach and how to contain the damage.

> *This view was compelling because dealing with content requires value judgments as to the legality or legitimacy of information, which interferes with freedom of speech online.*



The MITRE ATT&CK Enterprise Framework – screenshot from MITRE ATT&CK Navigator [5] showing (from left to right) the stages of a cyber attach (kill chain) and detailing techniques (in the columns) to carry out the stages

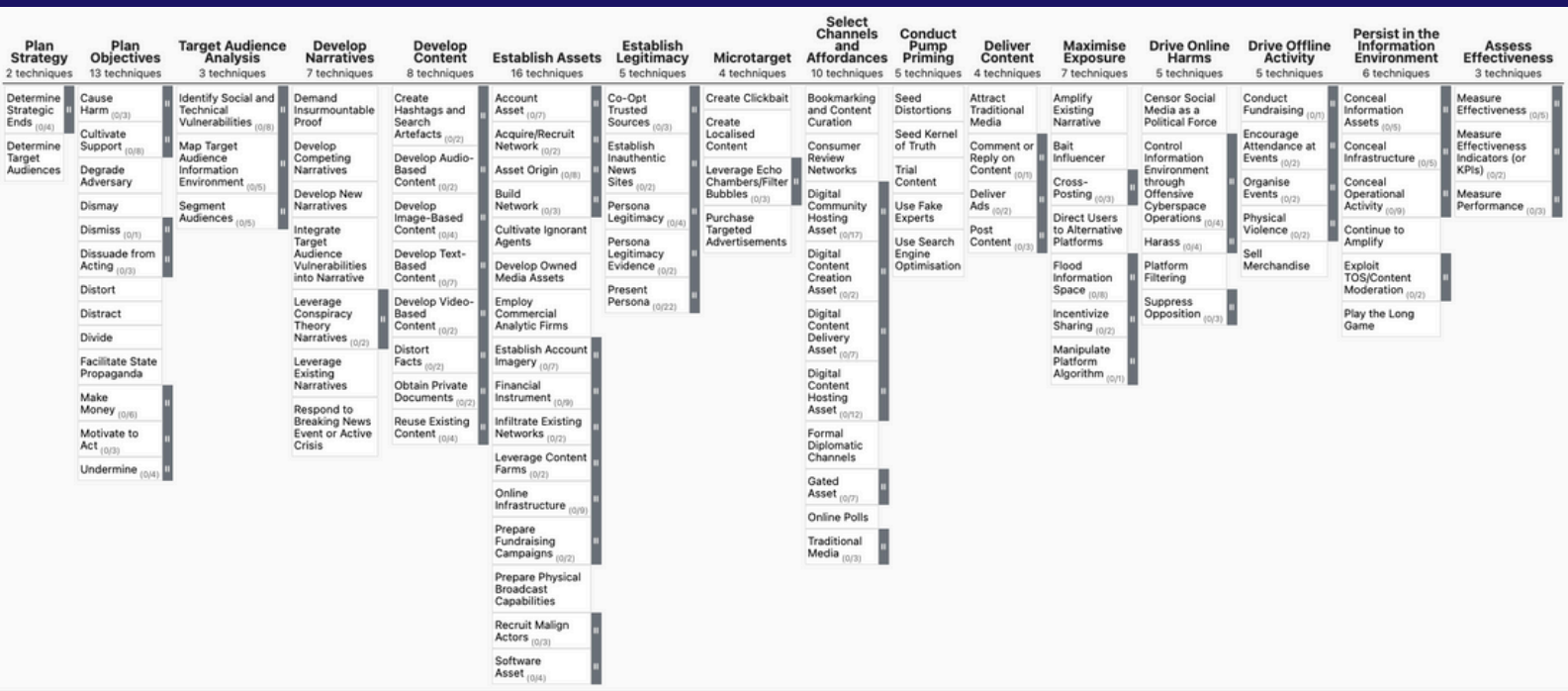
From cybersecurity 'kill chains' to information operations 'kill chains'

Cybersecurity policy and tradecraft have been careful in dealing with illegal content online. The prevailing view was that cybersecurity policy, cybersecurity tradecraft and specifically national Computer Security Incident Response Teams (CSIRTs) should not deal with illegal content. [6] This view was compelling because dealing with *content* requires *value judgments as to the legality* or legitimacy of information, which interferes with freedom of speech online. In addition, it requires *non-technical tools and skills*, thus not fit for the cybersecurity tradecraft. As a result, cybersecurity professionals have not focused on content, except when such content is part of the *kill chain*, such as social engineering or phishing.

Yet, the growing risk from malicious information operations, which include more and more both technical and content level tools, raise the question whether a more nuanced approach should be developed.

DISARM Framework

The Disinformation Analysis and Risk Management (DISARM) Framework serves as a potential middle ground because it aims to provide a common language for *documenting and analysing indicators of influence operations*, rather than just focusing on content including disinformation campaigns. In this sense, it follows the cybersecurity technical information sharing mindset.



The DISARM Framework – screenshot from DISARM showing (from left to right) the stages of an influence operation (kill chain) and detailing techniques (in the columns) to carry out the stages [7]

The framework has three important contributions in this area, which will be briefly described. The first is its *structured description of information dissemination techniques* and the development of a *disinformation kill chain*. The second, based on the *disinformation kill chain*, is a collection of *Disinformation Tools Techniques and Practices*, somewhat similar to the MITRE ATT@CK Framework. DISARM includes a *'Red Framework'* for describing adversary tactics and techniques and a *'Blue Framework'* for documenting defensive measures. The third is its role in support of operationalising policy in this area, such as the EU Digital Services Act requirements and the EU Foreign Information

and Manipulation (FIMI) framework to combat disinformation. These contributions will be elaborated briefly below to highlight the potential role of the cybersecurity community and its existing collaboration frameworks to deal with disinformation.

> *While there isn't a perfect parallel to MITRE ATT&CK for disinformation campaigns yet, DISARM offers valuable tools for understanding, analysing and countering disinformation.*

Structured description of the 'disinformation kill chain'

As part of the framework, a more detailed analysis was conducted to describe common mechanisms and techniques of *digital content distribution* in platform, thus unpacking the *disinformation kill chain*.

By clearly describing the *disinformation kill chain*, the framework highlights that there are technical and operational steps taken by malicious actors that are preliminary to the distribution of content. Such steps, as *creating an online identity or presence*, are detached from content and can indicate malicious activity. Focusing on these steps can support *identifying and blocking* attempted manipulations in information dissemination frameworks. [8]

Based on the *disinformation kill chain*, DISARM provides a structured matrix that supports identification and communication about disinformation operations. [9] While there isn't a perfect parallel to MITRE ATT&CK for disinformation campaigns yet, DISARM offers valuable tools for understanding, analysing and countering disinformation. A shared taxonomy and information sharing can support public-private and private-private information sharing to detect and block disinformation campaigns.

Importantly, it also serves to highlight the role of platform content dissemination and amplification mechanisms in the exposure of content. Platforms protect their *marketplaces of ideas* not only through (the more sensitive) *content moderation mechanisms*, but by monitoring and sharing information about *inauthentic behavior*. Such practices should be encouraged and enhanced by the cybersecurity community and informed by developed cybersecurity information sharing practices.

Supporting policy goals and policy support for the role of information sharing

The EU has taken a leading role globally in promoting a safer digital space with the EU Digital Services Act [10] and its FIMI (Foreign Information Manipulation and Interference) framework. [11] In both these frameworks there is an important role for harmonised information sharing about disinformation campaigns.

The European Commission recently endorsed the *Code of Practice on Disinformation* under the Digital Services Act (DSA). The *Code of Practice on Disinformation* sets out commitments for online platforms to tackle disinformation and includes *specific commitments* in this area. Under Title IV of the *Code Integrity of Services*, the Code (under Commitment 14) calls for *"Common understanding of impermissible manipulative behaviour"*. This section in turns refers to disinformation tactics, techniques and procedures (TTPs) frameworks. [12] In addition, using standard taxonomies improve the ability to under-stand and review platforms' actions in reducing the spread and impact of disinformation.

The EU FIMI framework also relates to technical information sharing, through an *emphasis on cooperation and situational awareness*. [13]

> *Like bug bounties and vulnerability disclosure programmes, community involvement makes platforms more resilient and more accountable. It improves the integrity of the infrastructure of the marketplace of ideas.*

Case study

A case in point are the recent findings as to foreign interference in the elections in Romania. [14] A group of researchers were able to clearly map a foreign interreference operation based on technical indicators. [15] These data and analysis suggests *"a pattern of coordinated amplification across various mediums and platforms, with messaging conduits spanning globally. The timing, scale and synchronised growth (in views, messages and reactions) highlight a strategically coordinated effort to increase visibility and public engagement."* [16] Such activity, when flagged, can be better monitored or even blocked by platforms in real time. In addition, a common taxonomy bridges the *cross-platform challenge*, in which platforms block malicious behavior on their infrastructure, but cannot do so on other platforms. And even if platforms push back, the community is still capable of having a *technical discussion* about indicators and *distribution dynamics*. In this sense, platforms should be interested in such a discussion. Like *bug bounties* and *vulnerability disclosure programmes*, community involvement makes platforms more resilient and more accountable. It improves the *integrity of the infrastructure* of the *marketplace of ideas*.

Instead of conclusion, a role for the cybersecurity community

As the policy ecosystem and practice around *content moderation* becomes more conflated, the promise to focus on transparency and *preventing technical* manipulation of content distribution platforms grows. The EU policy environment is pushing platforms for more transparency and this can support better technical monitoring. [17] The cooperative, sometimes informal and bottom-up nature of the cybersecurity community and cybersecurity information sharing, can perhaps bridge some of the recent global governance and trans-Atlantic tensions in this area. Cybersecurity professionals have a crucial role to play. And if they rise to the challenge, they can promote the protection of a safer cyberspace, in which basic freedoms are safeguarded from malicious interference.

References

[1] This definition is taken from the reference in the Code of Conduct of Disinformation [as amended in October 2024], (https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation), Communication from the Commission to The European Parliament, the Council, the European Economic and Social Committee And the Committee of the Regions on the, European Democracy Action Plan (03 December 2020) COM(2020)790 final (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790).
Note that the EU External Action Service has a specific definition for "Foreign Information Manipulation and Interference" as follows: "a 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." (https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en)

[2] See for instance: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/
And more recently, in the Romanian election context (as will be discussed in the text):
Andra-Lucia Martinescu, Sorina Stallard, Alina Balatchi-Lupascu, Mihai George Forlafu & the Osavul Data Team: Yan Kurtov, Dmytro Bilash, Dmytro Plieshakov & Yevhen Popov, Networks of Influence: Decoding foreign meddling in Romania's elections: A collaborative investigation into disinformation campaigns and influence operations, December 2024 (https://fpc.org.uk/wp-content/uploads/2024/12/Networks-of-Influence-Decoding-foreign-meddling-in-Romanias-elections-2024.pdf), "Networks of Influence".

[3] For a critical view of this vision see: Amy Kapczynski, Freedom From the Marketplace of Speech, The Knight First Amendment Institute at Columbia University, 14.02.2022, https://knightcolumbia.org/blog/freedom-from-the-marketplace-of-speech

[4] By this we mean the endorsement by the EU commission of the integration of the voluntary Code of Practice on Disinformation into the Digital Services Act, see: EU Commission, Commission endorses the integration of the voluntary Code of Practice on Disinformation into the Digital Services Act, 13.02.2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_505

[5] MITRE ATT&CK Navigator - https://mitre-attack.github.io/attack-navigator/

[6] One of the seminal studies at the first wave of cybersecurity national policies warned policy makers from tasking national C-SIRTs with dealing with content. See: Tim Maurer, Mirko Hohmann, Isabel Skierka, and Robert Morgus, National CSIRTs and Their Role in Computer Security Incident Response, New America, 19.11.2015, https://www.newamerica.org/cybersecurity-initiative/policy-papers/national-csirts-and-their-role-in-computer-security-incident-response/. The authors write that: "Meanwhile, on the global level, there is significant disagreement over what constitutes a threat and what falls within the purview of an nCSIRT. In some authoritarian systems, a cybersecurity threat is not only an actor that could cause damage through malicious code, but also an individual who publishes content online" (at p. 14-15). As a result, they catalogue C-SIRT activity in this area as "political" and thus advise against tasking C-SIRTs' with dealing with content. (p. 26).

[7] DISARM Foundation, https://disarmfoundation.github.io/disarm-navigator/

[8] See for example the description from Meta's team about "coordinated inauthentic behavior". Ben Nimmo and Eric Hutchins, Phase-based Tactical Analysis of Online Operations, The Carnegie Endowment for International Peace, 16/03/2023, https://carnegieendowment.org/research/2023/03/phase-based-tactical-analysis-of-online-operations?lang=en

[9] Sánchez González, Felipe. "DISINFOX: A Threat Intelligence sharing platform for disinformation incidents." (2025).

[10] EU Commission, Digital Services Act, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

[11] EU External Action Service, Tackling Disinformation, Foreign Information Manipulation & Interference, https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en

[12] See Recital d: "Relevant Signatories aim to collaborate together in drawing up a comprehensive list of shared terminology of impermissible manipulative behaviours and practices, which should periodically be amended in light of the latest evidence on the conducts and tactics, techniques and procedures (TTPs) employed by malicious actors, in particular to the AMITT Disinformation Tactics, Techniques and Procedures Framework. Such collaboration could take place in the framework of the Permanent Task-force set by this Code."
Note: The AMITT framework was merged into DISARM, as explained in the DISARM website. https://www.disarm.foundation/brief-history-of-disarm

[13] See: EU External Action Service, Strategic Communication and Foresight (SG.STRAT) Data Team, How to Detect and Analyse Identity-Based Disinformation/FIMI, A Practical Guide to Conduct Open-Source Investigations. November 2024, https://www.eeas.europa.eu/eeas/how-detect-analyse-identity-based-disinformationfimi-practical-guide-conduct-open-source_en, p. 4-5.

[14] See: Paula Erizanu, Romania's 'rigged' election shows Europe the dangers of Russian disinformation, The Guardian, 11.12.2024, https://www.theguardian.com/commentisfree/2024/dec/11/romania-presidential-election-russia-disinformation-europe

[15] See "Networks of Disinformation", p. 12: "Based on indicators of compromise (IOCs) embedded in the information threat detection platform, we identified a vast destabilisation arsenal that included 144 actors/networks specialised in disinformation campaigns and 469 pertaining to influence operations, with one such outfit also placed under international sanctions." It should be noted that the authors explain that some of the indicators are content related in the sense that they deal with content features and narratives. See footnote 31 on p. 12. See also the graph on p. 18 displaying "the networked component of four Romanian language channels and accounts (labels in red) and how they link to Russian-affiliated influence and disinformation vectors, many of which are based in Europe."

[16] See "Networks of Disinformation", p. 17.

[17] See above about the EU commission endorsement of the Code of Conduct, and also: David Sullivan, Systemic Risk Assessments Hold Clues for EU Platform Enforcement, Lawfare, 11.02.2025, https://www.lawfaremedia.org/article/systemic-risk-assessments-hold-clues-for-eu-platform-enforcement

Cybersecurity – information sharing and cooperation networks – and fighting disinformation – a bottom-up approach to reclaim safety in cyberspace

Amit Ashkenazi

EU CybetNet Expert Series, No 1, 2025

EU CyberNet

Funded by the European Union