Source Appendix

For: “Democracy is Critical Infrastructure now” by Robert F. Tjón, May 2026

Purpose: Concrete source material for the examples mentioned in the essay, plus the sources used for the factual checks.

Editorial note: Some examples below are publicly attributed to Russian or Russian-linked actors; others are included as examples of the type of incident mentioned in the prose. Where attribution is unclear or disputed, this is stated explicitly.

1. Concrete examples behind the incident phrases

A cyber intrusion that can be denied

Bundestag / German political targets and APT28. Germany publicly attributed repeated malicious cyber activity to Russian state-sponsored actors and APT28; cyber attribution is inherently difficult, which is why such operations often live in the grey zone.

- **Source:** German Federal Ministry of the Interior / Federal Government attribution, 3 May 2024
- **URL:** https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html

A cyber intrusion that can be denied — technical/legal context

Useful legal and technical case summary of the 2015 Bundestag hack and attribution issues.

- **Source:** CCDCOE Cyber Law Toolkit — Bundestag Hack (2015)
- **URL:** https://cyberlaw.ccdcoe.org/wiki/Bundestag_Hack_%282015%29

A local-looking news site that did not grow locally

Doppelganger / cloned or spoofed European news sites. The German Foreign Office and independent researchers describe Russian-linked networks using fake or cloned media pages to push pro-Kremlin narratives.

- **Source:** German Federal Foreign Office technical report on Doppelganger, 5 June 2024
- **URL:** https://www.auswaertiges-amt.de/resource/blob/2682484/2da31936d1cbeb9faec49df74d8bbe2e/technischer-bericht-desinformationskampagne-doppelgaenger-1--data.pdf

A local-looking news site that did not grow locally — investigation

Investigative reporting on how Doppelganger infrastructure helped spread propaganda via fake websites.

- **Source:** Correctiv — “Inside Doppelganger”, 22 July 2024
- **URL:** https://correctiv.org/en/fact-checking-en/2024/07/22/inside-doppelganger-how-russia-uses-eu-companies-for-its-propaganda/

A railway cable cut at the wrong moment

Northern Germany rail sabotage, October 2022. Cables vital for railway communication were intentionally cut; authorities called it sabotage, while the perpetrator and motive were not publicly identified as Russian. This is included as an infrastructure-vulnerability example, **not as a proven Russian operation**.

- **Source:** Reuters — “Malicious and targeted sabotage halts rail traffic in northern Germany”, 8 October 2022
- **URL:** https://www.reuters.com/world/europe/rail-northern-germany-standstill-due-technical-issue-2022-10-08/

A railway cable cut at the wrong moment — additional reporting

Additional contemporaneous reporting on the disruption and investigation.

- **Source:** RFE/RL — German Rail Operator DB Blames “Sabotage”, 8 October 2022
- **URL:** https://www.rferl.org/a/german-rail-operator-blames-sabotage-train-stoppage/32071278.html

A leaked conversation, twisted just enough to poison trust

German Taurus leak, March 2024. A recording of German officers discussing Ukraine support was published by Russian media; Germany described it as part of Russia’s information war aimed at creating division.

- **Source:** Reuters — Germany accuses Russia of information war after military recording, 3 March 2024
- **URL:** https://www.reuters.com/world/europe/germany-accuses-russia-information-war-after-military-recording-2024-03-03/

A leaked conversation — additional reporting

Associated Press report on Defence Minister Boris Pistorius’s assessment of the leak.

- **Source:** AP — German defence minister says leaked audio is part of Russia’s information war, 3 March 2024
- **URL:** https://apnews.com/article/8acc3ca7c858ff07085f643ec2da20ff

A drone near sensitive airspace

Latvia and Romania drone breaches / fragments, September 2024. NATO members reported Russian drones breaching airspace or fragments following attacks on Ukraine. NATO officials condemned the incidents while noting no public indication of a targeted attack against NATO.

- **Source:** Reuters — NATO members Romania, Latvia report Russian drones breach airspace, 8 September 2024
- **URL:** https://www.reuters.com/world/europe/romania-searching-possible-drone-fragments-after-russian-attack-ukraine-2024-09-08/

A drone near sensitive airspace — Latvia case

Latvian military statement reported by Reuters that the Russian drone carried explosives.

- **Source:** Reuters — Russian drone that crashed in Latvia carried explosives, 9 September 2024
- **URL:** https://www.reuters.com/world/europe/russian-drone-that-crashed-latvia-carried-explosives-latvian-military-says-2024-09-09/

A rumour released when an election is already tense

European election / French examples. Reuters reported Russian-linked disinformation before the 2024 European elections, including a fake French government website alleging mass call-ups to fight in Ukraine and amplification of the Paris bedbug scare.

- **Source:** Reuters — EU struggles to counter Russian election disinformation, 2 June 2024
- **URL:** https://www.reuters.com/world/europe/european-election-eu-struggles-counter-russian-disinformation-2024-06-03/

A rumour released when an election is already tense — earlier French example

Earlier French presidential-campaign example: Macron's campaign said Russian media and online activity spread rumours and fake news in 2017.

- **Source:** Reuters — French election contender Macron is Russian "fake news" target, 13 February 2017
- **URL:** https://www.reuters.com/article/world/french-election-contender-macron-is-russian-fake-news-target-party-chief-idUSKBN15S180/

Not every incident listed above was a confirmed Russian operation. The railway-cable example, in particular, is best used as a concrete illustration of infrastructure vulnerability and uncertainty, ***not as proven Russian sabotage.***

2. Sources used for the factual checks

Russia / NATO confrontation as planning scenario

Estonian intelligence and Reuters reporting that Russia is preparing for possible confrontation with the West within the next decade; use as scenario, not certainty.

- **Source:** Reuters — Russia preparing for military confrontation with West, says Estonia, 13 February 2024
- **URL:** https://www.reuters.com/world/europe/russia-preparing-military-confrontation-with-west-says-estonia-2024-02-13/

Estonian intelligence primary context

Estonian Foreign Intelligence Service annual report context on Russian threat perceptions and the risk to NATO over time.

- **Source:** Estonian Foreign Intelligence Service — International Security and Estonia 2024, Foreword
- **URL:** https://raport.valisluureamet.ee/2024/en/foreword/

EU election interference

European Parliament motion on alleged Russian interference in the European Parliament and upcoming EU elections.

- **Source:** European Parliament — B-9-2024-0266, 22 April 2024
- **URL:** https://www.europarl.europa.eu/doceo/document/B-9-2024-0266_EN.html

Foreign interference pattern in European elections

Context on bribery, information manipulation and foreign interference around European elections.

- **Source:** German Marshall Fund — Bribes and Lies: Foreign Interference in Europe in 2024, 24 July 2024
- **URL:** https://www.gmfus.org/news/bribes-and-lies-foreign-interference-europe-2024

France nuclear fleet correction

Primary database showing France with 57 nuclear power reactors in operation.

- **Source:** IAEA PRIS — France country details
- **URL:** https://pris.iaea.org/pris/CountryStatistics/CountryDetails.aspx?current=FR

Flamanville-3 detail

IAEA PRIS reactor detail page for Flamanville-3, used to confirm the change behind the 57-reactor figure.

- **Source:** IAEA PRIS — Flamanville-3 reactor details
- **URL:** https://pris.iaea.org/PRIS/CountryStatistics/ReactorDetails.aspx?current=873

Belgium nuclear correction

European Commission approval of Belgian state aid for ten-year extension of Doel 4 and Tihange 3.

- **Source:** European Commission — State aid approval for Belgian nuclear reactors, 20 February 2025
- **URL:** https://ec.europa.eu/commission/presscorner/detail/en/ip_25_565

Belgium nuclear reporting

Reuters reporting on EU approval of aid to extend Engie/Electrabel reactors Doel 4 and Tihange 3.

- **Source:** Reuters — EU approves state aid to extend life of Engie's Belgian nuclear reactors, 21 February 2025
- **URL:** https://www.reuters.com/business/energy/eu-regulators-clear-aid-engies-belgian-nuclear-reactors-2025-02-21/

France cyber threat level

ANSSI's 2025 cyber threat overview: high threat level, blurred boundaries between state actors and cybercriminals.

- **Source:** ANSSI — Cyber Threat Overview 2025
- **URL:** https://cyber.gouv.fr/en/publications/cyber-threat-overviews/cyber-threat-overview-2025/

France cyber threat report PDF

Detailed ANSSI/CERT-FR PDF threat overview used for state-actor and critical-system context.

- **Source:** CERT-FR / ANSSI — Cyber Threat Overview 2025 PDF
- **URL:** https://cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-003.pdf

Belgium / NATO institutional geography

Official SHAPE site for NATO Allied Command Operations headquarters.

- **Source:** NATO SHAPE — official website
- **URL:** https://shape.nato.int/

SHAPE in Mons, Belgium

U.S. Mission to NATO explainer identifying SHAPE as located in Mons, Belgium.

- **Source:** U.S. Mission to NATO — Supreme Headquarters Allied Powers Europe (SHAPE)
- **URL:** https://www.usanato.army.mil/About-Us/Articles/Article/1513239/supreme-headquarters-allied-powers-europe-shape/

European-election information operations

European Commission memo summarizing known information interference operations during the 2024 European Parliament elections.

- **Source:** European Commission — Memo: Known information interference operations during EP elections, 11 October 2024
- **URL:** https://ec.europa.eu/commission/presscorner/api/files/attachment/879707/Memo%20-%20Known%20information%20interference%20operations%20during%20EP%20elections.pdf

Foreign electoral interference toolbox

APPF / European Parliament study describing financial, cyber and information manipulation tools used in electoral interference.

- **Source:** APPF — Foreign electoral interference affecting EU democratic processes
- **URL:** https://www.appf.europa.eu/cmsdata/277388/Foreign%20electoral%20interference%20affecting%20EU%20democratic%20processes.pdf

Publication caution

Not every incident listed above was a confirmed Russian operation. The railway-cable example, in particular, is best used as a concrete illustration of infrastructure vulnerability and uncertainty, ***not as proven Russian sabotage.***

AI Disclosure: My work utilizes artificial intelligence for data synthesis and structural mapping. Please note that AI-generated insights may occasionally contain inaccuracies; readers are encouraged to verify critical information. All conclusions and final editorial decisions remain the original work of Robert F. Tjón.