The challenge of post-truth: the impact of digital militias and disinformation on police intelligence activity and prospects for the critical curation of information.
The post-truth challenge: the impact of digital militias and disinformation on police intelligence activities and perspectives for critical information curation

Jorge Magalhães do Carmo - Bachelor of Laws from the Metropolitan Faculty of Manaus –
FAMETRO; Specialist in Constitutional Law and Administrative Law from the Dom Alberto Higher Education Center - DOM
ALBERTO; Cadet of the Military Police of Amazonas and Bachelor's student in
Public Security and Citizenship at the State University of Amazonas – UEA; Lattes CV: http://lattes.cnpq.br/6027924121344463 ;
Lattes ID: 6027924121344463; https://orcid.org/0009-0009-8317-2388 ; Contact:
jorgemagalhaesdc@gmail.com

Kristorferson Almeida do Rêgo - Cadet of the Military Police of Amazonas. Bachelor's degree in Public and Citizen Security from the State University of Amazonas –
https://lattes.cnpq.br/4078604726881272 Contact: kr.asafe.noah.pedro@gmail.com

Yracles da Silva Rodrigues - Bachelor's degree in Public and Citizen Security from UEA, Bachelor of Law from UNIFACISA,
Specialist in Public Security from Faculdade Focus. - Lattes CV: https://lattes.cnpq.br/3163889181737429

Contact: yracles@gmail.com

Flávio Carvalho Cavalcante - PhD candidate in the Postgraduate Program in Environmental Sciences and Sustainability in the Amazon (PPGCASA) at the Federal University of Amazonas. Master's degree in Public Security, Citizenship and Human Rights from the Postgraduate Program in Public Security (PPGSP) at the State University of Amazonas (UEA). Specialist in Strategic Management in Public Security. Specialist in Public Security Intelligence from the Ministry of Justice and Public Security/National Police Agency (ANP-PF). Specialist in Public Management Applied to Security from the State University of Amazonas (UEA). Specialist in Public Security and Police Intelligence from UNIC/LITERATUS. Specialist in Military Law from UNINORTE. Specialist in Legal Sciences from the University of São Paulo City (UNICID).

Holds a degree in Public Security from the State University of Amazonas - UEA. Bachelor of Laws from the University of São Paulo - UNICID. Is a member of the research group "Subjects, Actions and Perceptions: Research Group on Violence and Conflict", at the Federal University of Acre. Currently an Officer in the Military Police of the State of Amazonas, working in Intelligence and Criminal Investigation (MPAM). Has experience in the areas of Management, Administration, Public Security Intelligence, Knowledge Management and Criminal Analysis, with an emphasis on STRATEGIC MANAGEMENT IN PUBLIC SECURITY.

Summary

This article analyzes the operational and analytical impacts that digital militias and systematic disinformation impose on police intelligence agencies in Brazil, contextualizing this contemporary threat within the paradigm of intelligence-led policing. Starting from the origins and theoretical model of this police approach, the study problematizes how organized disinformation has ceased to be mere opinion and has become a tool for institutional destabilization and obstruction of justice, demanding an adaptation of intelligence processes. Using the methodology of bibliographic review and document analysis, based on official doctrines, specialized international literature, and emblematic cases, the work explores the convergence between the traditional model of interpreting the criminal environment and the need to filter a hostile informational ecosystem. It concludes...

Modern police intelligence must evolve into a practice of critical information curation, integrating *Open Source Intelligence* (OSINT) techniques, counterintelligence, strategic communication, and inter-institutional cooperation to protect the decision-making process and the democratic rule of law itself against digital cognitive warfare.

Keywords: Intelligence-led policing. Digital militias. Disinformation.

1

Abstract

This article analyzes the operational and analytical impacts that digital militias and systematic disinformation impose on police intelligence agencies in Brazil, contextualizing this
contemporary threat within the paradigm of intelligence-led policing. Starting from the origins and theoretical model of this police approach, the study problematizes how organized disinformation has ceased to be mere opinion and has become a tool for institutional destabilization and obstruction of justice, demanding an adaptation of intelligence processes.
Using the methodology of bibliographic review and document analysis, based on official doctrines, specialized international literature, and emblematic cases, the work explores the convergence between the traditional model of interpreting the criminal environment and the need to filter a hostile informational ecosystem. It concludes that modern police intelligence
must evolve into a practice of critical information curation, integrating Open Source Intelligence
(OSINT) techniques, counterintelligence, strategic communication, and interinstitutional cooperation to protect the decision-making process and the democratic rule of law itself against digital cognitive warfare.

Keywords: Intelligence-Driven   Policing.   Digital   Militias.   Misinformation. Counterintelligence.

Introduction

This article is timely, given that policing is currently undergoing a

a period of significant change in both operational tactics and structures.

Organizational. New ideas in crime reduction and changes in police strategies.

Short- and long-term plans are underway. Intelligence-led policing.

This represents a recent approach and is one of the most prevalent of the current "changes in

"philosophy of crime control and in police practice" (MAGUIRE, 2000). Surprisingly,

Given the wide distribution of the term, there is still considerable...

confusion regarding its true meaning, both for line officers of

both in front of and for police management (RATCLIFFE, 2002b).

The landscape of threats to public safety has undergone a profound transition, migrating

from predominantly physical actions to a hybrid domain where cybernetic and physical actions are present.

Informational arenas are central stages. In this new environment, the war for narratives and manipulation take center stage.

Social perception has become a tool as impactful as conventional weapons.

Public Security Intelligence (PSI) activity, whose core is the production of knowledge.

strategic for assisting in the prevention and repression of illicit activities (BRAZIL, 2016), it is seen

confronted with a diffuse and complex adversary: digital militias and the machine of

systematic misinformation.

The central problem lies in the fact that organized disinformation transcends the

It is not the realm of mere opinion or legitimate political debate. It is being used *maliciously.*

specifically designed to destabilize institutions, obstruct justice, and protect organizations.

2

criminal and undermine public trust in state institutions. This phenomenon is characterized, in

words from the National Public Security Intelligence Policy (PNISP), a clear "action

contrary to public safety in cyberspace" and "action contrary to the Democratic State"

of Law" (BRAZIL, 2021a, p. 10), requiring a proportional response from the state apparatus.

This article has a twofold objective: first, to revisit and detail the principles and the

intelligence-led policing model as established by Ratcliffe (2003) and

internationally widespread; secondly, to analyze the concrete impacts of the new modality.

The threat posed by digital militias imposes a significant burden on police intelligence activities.

The aim is to investigate how the *modus operandi* of these groups contaminates sources.

It overloads analytical cycles and undermines institutional credibility, demanding a

doctrinal and operational restructuring of intelligence agencies within the paradigm of

Intelligence-led policing. The analysis is based on a literature review.

original, in the National Doctrine of Public Security Intelligence (DNISP), in the PNISP, in

specialized literature and emblematic cases, such as the attacks of January 8, 2023 in

In Brazil, which highlighted the materialization of informational risk.

2. Intelligence-led policing in cyber-cognitive warfare

To understand the scope of the current challenge, it is essential to define the evolution of

central concept. Intelligence-led policing entered the police lexicon around

from the early 1990s, originating in the United Kingdom, in response to rising crime and

pressures for efficiency (GILL, 1998).

His goal was to shift the focus from the crime *itself* to the active criminal, directing

resources more effectively. The UK National Intelligence Model, for example, focused-

whether it involves targeting offenders, managing hotspots, investigating linked crime series and

Apply preventive measures (NCIS, 2000). This refers to the "application of intelligence analysis."

criminal law as an objective decision-making tool, in order to facilitate the reduction and

crime prevention through effective police strategies and external partnership projects

extracted from a body of evidence" (RATCLIFFE, 2003, adapted).

Regarding the importance of post-truth in the context of conflicts, PINHEIRO teaches,

AGUIAR, LIMA (2019, p.775) that:

> It is an element that has proven to be crucial, both in resolving conflicts
> and in creating them. Annually, the Oxford Dictionary, a department of
> the University of Oxford responsible for publishing...

3

> From English dictionaries, a term in the English language is chosen as the word of the year. In 2016, the selected term was "post-truth". Post-truth is a term used to describe a time when "circumstances in which objective facts have less influence in shaping public opinion than appeals to personal beliefs and emotions".

Furthermore, PINHEIRO, AGUIAR, LIMA (2019, p. 776) mentions masterfully that:

> And as is to be expected from an infectious disease (KUCHARSKI, 2016), post-truth hitched a ride on the red blood cells of liquid modernity, where the essential It is the movement of information regardless of its veracity or convenience (BAUMAN, 1999), and it has been transmitted through the veins of globalization until it reached Brazil, making an analysis of its effects necessary, since it is not a problem of underdeveloped countries but rather a global ill, which has shown itself to be similar to those of the United Kingdom and the United States (SOUZA, 2017 and TARDÁGUILA, 2018).

However, the criminal environment that the police must interpret has suffered a Radical expansion. It's no longer just about a physical environment or criminal networks. traditional. The "criminal environment" in the 21st century actively includes an ecosystem informational where malicious actors, including digital militias, operate to distort The reality. The term refers to organized groups that act in a coordinated manner and, often Sometimes, it becomes professionalized in the digital environment, using structures that simulate the appearance of digital media. legitimate for disseminating false (fake *news),* manipulated, or biased content on a mass scale with political, ideological or criminal objectives (BRAZIL, 2023 – CPMI of the Acts of 8 of January).

In this context, it is crucial to differentiate between *misinformation and disinformation.* While... Secondly, it can be the unintentional dissemination of incorrect information; misinformation is... characterized by intent *(malice).* It is a "manipulation strategy". "informational" where fake news is manufactured and systematically spread to "generate confusion between fact and opinion" and achieving predetermined goals, setting up true psychological operations in the digital space (SILVA FILHO, 2024). This intentionality It is malevolent that it elevates the phenomenon to the category of a threat to public safety and a legitimate object. from intelligence activity, requiring that the intelligence-led policing model be expanded to incorporate analysis and counter-attack against this new layer of threat.

4

3. Modus operandi of digital militias and the contamination of the intelligence cycle.

The effectiveness of digital militias lies in a sophisticated operational architecture that

This architecture directly attacks the pillars of intelligence-led policing.

It rests on three interconnected pillars that undermine the traditional process. First, the

technical infrastructure, which uses *bots,* click farms, and targeting algorithms to

to exponentially amplify the reach of false narratives. As demonstrated in the Report

Regarding the Parliamentary Commission of Inquiry into the Acts of January 8th, the speed and scope of the falsehoods far surpass the findings of the Parliamentary Commission of Inquiry into the Acts of January 8th.

those of true information (BRAZIL, 2023), creating an artificial volume that

It overloads the collection systems.

Thus, Almeida (2025, p. 32) asserts this when he states that:

> It is assumed that the police officer should store data collected by the agency.
> local intelligence, moreover, requires that certain data be
> subjected to processing and indexing procedures, if such
>
> data is stored and processed on the work computer of
> police, despite the information control guidelines implemented in
> On the network, the control of protected data becomes more comprehensive when
> performed on a specific server that is properly configured for that purpose.
> purpose. This approach not only optimizes the working time of
> agent, but it also reduces the costs associated with deploying multiple
> machines for processing in numerous units, in favor of a single
> Interconnected server structure. This allows police officers access
> client-server, as mentioned earlier. Furthermore, it facilitates
> that, at any time or on any computer on the institution's network
> police officer, it is possible to access in order to update, modify or collect
> information that has already been processed. Thus, the computer used regularly
> The agent would merely serve as an access tool, and nothing more.
> as a device for processing and storing crucial data
> for public safety.

Secondly, the exploration of echo chambers. The fragmentation of public space into

homogeneous ideological bubbles, facilitated by platform algorithms, allow that

False narratives circulate and reinforce each other without critical counterpoint. For police intelligence,

This means that data collected from open sources (OSINT) may already be severely compromised.

distorted, representing not social reality, but a fabricated and amplified reality.

digitally (SILVA FILHO, 2024).

Finally, a cognitive war is being waged. The messages are carefully crafted.

built to trigger primary emotional responses—fear, hatred, tribalism—inhibiting the

Rational critical thinking. This attack is doubly dangerous: it targets both the population, and

5

manipulating their perception of the police and the justice system, as well as the analysts and decision-makers themselves

decision, potentially leading to cognitive biases in the analysis or decision paralysis due to fear.

of media retaliation.

The impact of this ecosystem on intelligence activity is multifaceted. The first

The affected pillar is the reliability of the sources and the contamination of the production cycle. The analyst,

which relies on the collection and sorting of data from diverse sources, runs the constant risk of

to use information that has been "planted" or distorted by disinformation campaigns.

Fabricated data can be deliberately inserted to divert resources.

investigative actions, protecting criminals or incriminating innocent people, constitute an act of counter-

intelligence on the part of adversaries. The ABIN Doctrine warns that the protection of

Knowledge and detection of interference are primary functions of counterintelligence.

(BRAZIL, 2023).

The second pillar is information overload or *infoxication.* The massive volume and

The speed at which false content spreads generates deafening noise. Analysts,

Often with lean teams, they can be overwhelmed by the work of verifying a myriad of...

of dubious information, delaying the processing of genuinely relevant data.

As Espuny (2021) points out, the "data storm" can cause capabilities

analytical capabilities fall behind data collection capabilities, compromising the principle of

Timeliness, the production of knowledge at the opportune moment for decision-making.

Finally, digital militias promote a direct attack on institutional credibility.

Coordinated campaigns are specifically aimed at demoralizing intelligence agencies.

Public prosecutors, police and their agents. The narrative of "political persecution" or

"Incompetence" aims to invalidate future operations, evidence, or reports in the eyes of the public.

intelligence. This attack undermines the authority of institutions and can intimidate public servants.

weakening the entire public security and justice system, eroding the very capacity of

The police's role in "influencing decision-makers" is a crucial step in Ratcliffe's model.

4. Contingencies for disinformation in the intelligence process

The classic model of intelligence-led policing, as represented

In the literature (RATCLIFFE, 2002b), it is a process that begins with the interpretation of

In the criminal environment, the focus shifts to producing intelligence that should influence decision-makers.

decision-making, so that these can finally have a positive impact on the criminal environment. However, this model does not explicitly consider a contaminated information environment. Digital militias operate to corrupt each of these structures, demanding a defensive expansion of the model.

In the phase of interpreting the criminal environment, analytical ability is seriously important. compromised when a significant portion of the available data, especially from sources open (OSINT), is deliberately false. Therefore, a critical subfunction at this stage must be Validation and counterinformation screening. Systems and analysts need tools and Training to identify *bots, deepfakes,* astroturfing patterns, and coordinated campaigns. Cooperation with cybersecurity and *fact-checking* experts becomes essential. Infoxication is a tactic of the adversary; against it, the police need curation of sources and assisted technological screening.

In producing intelligence, the analyst can no longer simply synthesize data; they must to qualify them with a seal of reliability that takes into account the health of the ecosystem. The intelligence product should, when relevant, contain an informational overview of that topic. assessment of the presence and potential impact of related disinformation campaigns To the target.

In the stage of influencing decision-makers, police intelligence based on Evidence now competes with viral narratives that are simple and emotionally charged. They also reach commanders, public managers, and partners. The intelligence unit, Therefore, you must develop strategic communication skills.

Your product cannot be just a technical report; it must, when necessary, be accompanied by materials that debunk false narratives in advance and prepare the decision-makers to confront the misinformation that will inevitably arise. External partners, such as Municipal authorities or community leaders are especially vulnerable and should be alerted and trained against these threats.

Finally, when impacting the criminal environment, operational planning must include An integrated communication plan. This involves selective transparency to occupy the space. informational with facts, real-time monitoring of response narratives and capability a quick correction of falsehoods. Without it, the tactical success of an operation can be nullified by A narrative failure, eroding police legitimacy, a fundamental asset for effectiveness. long term (SCOTT, 1998).

The principle of proportionality (RATCLIFFE, 2002b) is further challenged. when police tactics are digitally distorted, requiring the police to prepare for

7

To publicly justify your actions in a clear and accessible manner.

5. The role of police intelligence in addressing

Faced with this asymmetrical threat, police intelligence cannot be passive. It must integrate specific information combat capabilities into its operational model.
A key tool is the strategic and forensic use of Open Source Intelligence.
(OSINT). More than just collecting data from the internet, it's about applying analytical methodology.
rigorous to monitor behavioral patterns of these networks, identify influencers-
Key tools include tracing the origin of campaigns and uncovering their financial or logistical connections.
(CEPIK, 2023).

Technology and Artificial Intelligence (AI) are emerging as indispensable allies.
However, they should be cautious. Tools for link analysis, data mining, and *bot* detection.
They can automate the identification of dissemination patterns and *clusters* of misinformation.
However, as the literature warns, AI also brings risks, such as the loss of human context.
and the generation of even more convincing false content (MARR, 2023). The human element-
Analytical analysis remains irreplaceable in the final interpretation and attribution of intentionality.

Integration with counterintelligence becomes imperative. The function of "protecting the
The action of interfering in the decision" (BRAZIL, 2023) is central. This involves protecting assets.
(agents, sources, methods), the critical communication infrastructures of the police and,
Primarily, protecting institutional image and credibility against fraudulent narratives. Actions
Counter-propaganda, based on truthful and transparent information, can be
necessary to deconstruct adverse narratives and protect the decision-making space, acting as
a barrier in the expanded model.

6. Ethical, legal, and organizational culture challenges

This more assertive approach in the digital environment raises complex dilemmas. The main one
It is about balancing the vigilance necessary to identify threats with guaranteeing freedoms.
Expression and privacy. Monitoring public networks to identify patterns.
Organized criminal activity is distinct from indiscriminate surveillance of citizens. The approach must be...
always based on law, with robust external oversight, to avoid repeating past abuses.

There is an urgent need for more robust and specific legislation. Although laws such as
Crimes against the Democratic Rule of Law (Law No. 14.197/2021) and against Organizations

8

Criminal offenses (Law No. 12.850/2013) can be applied, a clear definition of disinformation is necessary.

systematic and financed as a crime, whether against public administration or as an instrument

This would provide greater legal certainty to the investigations into organized crime.

Internally, police services face the challenge of a performance culture.

Pressure for quantitative metrics can divert attention from the necessary in-depth qualitative analysis.

to understand networks of influence (SCOTT, 1998). The evaluation of results should prioritize the

Crime prevention facilitated by disinformation and the neutralization of campaigns

Interference, and not just processing volumes.

Conclusion

The push for intelligence-led policing must be tempered by

Realistic expectations and adapted to new threats. The ability of the police to impact the level.

Crime prevention in society is limited, but gains are possible through collaboration with agencies.

external factors that hold the key to deeper causal factors (HEATON, 2000;

(WEATHERBURN, 2001). This conclusion remains valid, but requires expansion.

crucial. The "external agencies" with which the police must now collaborate include platforms

social media, technology companies, and fact-checking organizations. The

Intelligence sharing should include the exchange of data on campaigns.

malicious misinformation.

The post-truth era and the rise of digital militias are forcing a paradigmatic redefinition of...

Police Intelligence. It's no longer enough to simply collect and process data; it's necessary...

To become a critical curator of truth in a sea of manipulation. The ISP must evolve to

an activity that not only prevents physical crimes, but also identifies, neutralizes and...

protects it from informational attacks designed to paralyze and delegitimize it.

Effective action will require multi-sectoral and international cooperation, given that

The transnational nature of disinformation platforms and networks. Investment in

Continuous training of analysts, equipping them with knowledge in psychology, communication,

Digital law and social media analytics is a strategic imperative. The model of

Intelligence-led policing, as conceived in the late 20th century, provides

a solid structure; it is up to the next generation of professionals to strengthen it for the challenges of...

In the 21st century, false ideas are the new weapons and analytical clarity is the main shield.

9

References

ALMEIDA, ANDRÉ MARCELO DE. *Use of computer network infrastructure, data processing and the implementation of artificial intelligence in local public security agencies.* In: ZOGAHIB, ANDRÉ LUIZ NUNES (org.). *Public security, citizenship and human rights: research, reports and reflections.* Ponta Grossa: Aya, 2024. p. 349.

AUSTRALIAN CUSTOMS SERVICE. *Intelligence doctrine.* Canberra: ACS, 2000.

AUDIT COMMISSION. *Helping with inquiries: tackling crime effectively.* London: HMSO, 1993.

BRAZIL. *National Doctrine of Public Security Intelligence (DNISP).* 4th ed. Brasília: Ministry of Justice; ABIN, 2016.

BRAZIL. *Decree No. 10,777, of August 24, 2021.* Approves the National Public Security Intelligence Policy (PNISP). Official Gazette of the Union: Brasília, 2021.

BRAZIL. National Congress. *Final report of the Joint Parliamentary Inquiry Commission (CPMI) on the Acts of January 8, 2023.* Brasília: National Congress, 2023.

BRAZIL. Brazilian Intelligence Agency. *Doctrine of Intelligence Activity.* Brasília: ABIN, 2023.

CEPIK, MARCO. *Espionage and democracy: agility and transparency as dilemmas in the institutionalization of intelligence services.* 2nd ed. Belo Horizonte: Fórum, 2023.

CHILVERS, M.; WEATHERBURN, D. *Operation and Crime Review panels: their impact on break and enter.* Crime and Justice Statistics Bureau Brief. Sydney: NSW Bureau of Crime Statistics and Research, 2001.

DUNNINGHAM, C.; NORRIS, C. *The detective, the snout, and the Audit Commission: the real costs in using informants.* Howard Journal of Criminal Justice, vol. 38, p. 67–86, 1999.

ECK, JE; SPELMAN, W. *Problem solving: problem-oriented policing in Newport News.* Washington, DC: Police Executive Research Forum, 1987.

ERICKSON, RV; HAGGERTY, KD *Policing the risk society.* Oxford: Clarendon Press, 1997.

ESPUNY, HERBERT GONÇALVES. *Public security intelligence: highlights of its practice.* In: BELIATO, ARACELI M. et al. (org.). *Police intelligence.* Mizuno Series. 2024. p. 156–168.

GILL, P. *Making sense of police intelligence? The use of a cybernetic model in analyzing information and power in police intelligence processes.* Policing and Society, vol. 8, p. 289–314, 1998.

GOLDSTEIN, HERMAN. *Problem-oriented policing.* New York: McGraw-Hill, 1990.

10

HEATON, R. *The prospects for intelligence-led policing: some historical and quantitative considerations.* Policing and Society, vol. 9, p. 337–356, 2000.

HER MAJESTY'S INSPECTORATE OF CONSTABULARY. *Policing with intelligence.* London: HMIC, 1997.

HER MAJESTY'S INSPECTORATE OF CONSTABULARY. *Northamptonshire Police: intelligence-led policing and proactive investigation of crime.* London: HMIC, 2001.
HER MAJESTY'S INSPECTORATE OF CONSTABULARY. *Bedfordshire Police: crime intelligence.* London: HMIC, 2002.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE. *Criminal intelligence sharing: a national plan for intelligence-led policing at the local, state and federal levels.* Alexandria, Virginia: COPS; IACP, 2002.

LAYCOCK, G. *Research for police: who needs it?* Trends and Issues in Crime and Criminal Justice, n. 211. Canberra: Australian Institute of Criminology, 2001.

MAGUIRE, M. *Policing by risks and targets: some dimensions and implications of intelligence-led crime control.* Policing and Society, vol. 9, p. 315–336, 2000.

MAGUIRE, M.; JOHN, T. *Intelligence, surveillance and informants: integrated approaches.* Police Research Group: Crime Detection and Prevention Series, no. 64, 1995.

MARR, BERNARD. *The 15 biggest risks of artificial intelligence.* Forbes Tech, 2023.

NATIONAL CRIMINAL INTELLIGENCE SERVICE. *The National Intelligence Model.* London: NCIS, 2000.

PAWSON, R.; TILLEY, N. *Realistic evaluation.* London: Sage, 1997.

PINHEIRO, J.; AGUIAR, D.; LIMA, A. *The influence of post-truth and liquid modernity on the consensual resolution of conflicts.* In: VIVAS, ALESSANDRA BENTES T. et al. (org.). *Interdisciplinarity of public policies.* Rio de Janeiro: Pembroke Collins, 2019. v. 1. p. 774–790.

RATCLIFFE, JH *Intelligence-led policing.* Canberra: Australian Institute of Criminology, 2003.

RATCLIFFE, JH *Policing urban burglary.* Trends and Issues in Crime and Criminal Justice, n. 213. Canberra: Australian Institute of Criminology, 2001.

RATCLIFFE, JH *Burglary reduction and the myth of displacement.* Trends and Issues in Crime and Criminal Justice, n. 232. Canberra: Australian Institute of Criminology, 2002.

RATCLIFFE, JH *Intelligence-led policing and the problems of turning rhetoric into practice.* Policing and Society, vol. 12, p. 53–66, 2002.

SCOTT, J. *Performance culture: the return of reactive policing.* Policing and Society, vol. 8, p. 269–288, 1998.

11

SHERMAN, LW et al. *Preventing crime: what works, what doesn't, what's promising.* Washington, DC: National Institute of Justice, 1998.

SILVA FILHO, MANUEL CAMILO DA. *Systematic disinformation and fake news by digital militias and their implications for intelligence activity.* In: BELIATO, ARACELI M. et al. (org.). *Police intelligence.* Mizuno Series. 2024. p. 180–196.

WEATHERBURN, D. *What causes crime?* Crime and Justice Bulletin, no. 54. Sydney: NSW Bureau of Crime Statistics and Research, 2001.

12