HADMÉRNÖK
VÉDELEMINFORMATIKA
21. évfolyam (2026) 3. szám 21–42.
DOI: 10.32567/hm.2026.3.2

Olga Lavro-Gazdag[1]

Doxxing as an Information Operation[2]

A Theoretical Synthesis and Classification Framework

Abstract

Doxxing is commonly defined as the intentional gathering and non-consensual public release of personal information online, with the aim of humiliating, intimidating, threatening, or punishing a target. Military doctrine defines information operations as activities intended to influence, disrupt, corrupt, or disable decision-making. Information operations may take place in the physical sphere (e.g. damaging communication cables) or in the cognitive dimension. The aim of this paper is to determine when doxxing is only a privacy issue and when it is functionally equivalent to an information operation. The literature shows that online harassment can lead to heightened distress, a state that may resemble post-traumatic stress disorder and cause interference across several domains of a person's life. The literature also documents behavioural change, such as self-censorship and withdrawal from social activities. Targeted doxxing has been documented against police and military personnel. Such acts can signal to members of the national bodies responsible for a society's security and safety that their work carries a high personal price. This broader interpretation of information operations renders the phenomenon intelligible beyond conventional military confrontation, in relation to the threat posed by non-state actors and hybrid threats, which are connected to society and to the diverse possibilities and freedoms of the information space in substantially wider ways. In peacetime, one of the greatest challenges is the use of various elements of information operations in many

[1] PhD student, Ludovika University of Public Service, Doctoral School of Military Sciences.

[2] Artificial intelligence (Claude Opus 4.8) was used in the preparation of this paper to improve language and to assemble the rubric table, the illustrative scoring table of the examples and the figure summarising how certain doxxing events evolve and become an instance of information operation.

parts of the world, among which numerous activities in cyberspace can be observed. The interpretation of doxxing as an information operation is one such case.

Keywords: doxxing, information operation, psychological operation, target degradation, cognitive effect, hybrid warfare, fear, technology-facilitated violence

Introduction

Doxxing of people working in national security has become a recurring threat across the globe. Recent high-profile incidents remind us that, where data protection, digital-footprint awareness, and mitigating measures are not applied, the scale and the consequences of doxxing can be devastating.[3]

Doxxing campaigns targeting soldiers, police officers, and special agents reveal a consistent pattern. The published – usually large – datasets are weaponised to threaten individuals and their families, and resorting to doxxing degrades operational security. For example, a website known as the "ICE List" reportedly published the identities of thousands of alleged ICE and Border Patrol personnel.[4] In Portland, anarchist-affiliated groups publicly posted the names, photographs, home addresses, and even images of the families of ICE agents. The U.S. Department of Homeland Security reported an approximately 700% increase in assaults on ICE personnel in that jurisdiction following such activity.[5] The data used in doxxing campaigns can come from manifold sources. So-called combolists, for instance, are sold on the deep and dark web. They contain names, usernames, telephone numbers and email addresses, and in some cases cleartext passwords, which can lead to further breaches. A determined threat actor can then conduct reconnaissance, which can be done easily in the online space by anyone with modest technical knowledge. Doxxed personnel may face physical danger (e.g. harassment and attacks) and operational degradation (e.g. reduced willingness to share intelligence or to serve in sensitive roles). Mitigating such a threat requires an integrated approach. First and foremost, the nature of doxxing itself must be studied.

The information environment is now a contested space. States, non-state actors, and ordinary online bystanders compete within it for attention and for influence over decisions. One keyword of this paper is fear – fear of what happens in the online sphere, whether through network intrusions via internet-connected devices or through the information uploaded online. Anxiety can arise because a person's personal data was released online, without consent, in order to cause harm. As one military historian observes, military action is driven either by commands grounded in fear or by moral and ethical values and goals.[6] Doxxing builds on fear: a published name, address, family relationship, or interest can be weaponised against a target. Doxxing began as hacker slang, from "dropping docs", when rival hacker groups sought to expose one another's identities. Today it is largely a privacy issue that may breach data protection law – in

[3] Kovács 2020.
[4] Putman 2026.
[5] U.S. Department of Homeland Security 2025.
[6] Boda 2018.

particular the European Union's General Data Protection Regulation (GDPR). Doxxing is the intentional release of an individual's personal information onto the internet by a third party, typically without consent and with the aim of humiliating, threatening, intimidating, or punishing the target.[7] The author distinguishes three forms: deanonymising (exposing the identity of a previously anonymous person), targeting (revealing otherwise obscured details such as a home address), and delegitimising (disclosing information meant to damage a person's credibility).[8]

Information operations are studied by military scholars, strategists and political scientists alike. In U.S. joint doctrine, an information operation is the disabling and altering of information in order to influence or disable the decision-making capabilities of the adversary while protecting one's own.[9] It is not a single weapon and may be insufficient on its own. Psychological operations, electronic warfare, and computer network operations are distinct fields that fall within information operations.

Doxxing has been reported in relation to military personnel: by publishing addresses, perpetrators sought to incite public fury and to provoke aggression against uniformed individuals.[10] Doxxing has also been described as a political harassment tactic used against police officers. Research indicates that the aim of such acts was to raise the transactional costs of protest policing so that officers refrain from volunteering.[11] These examples align with what an information operation is: doxxing here seeks to influence behaviours and perceptions. Moreover, if service members are intimidated through the publication of their information online, one possible outcome is that they leave the service. Deprived of their knowledge and skills, the decision-makers of the body may then make ill-informed decisions.[12]

This paper develops a theoretical framework for determining when doxxing can be classified as information or influence operations. It draws on published definitions and typologies of doxxing, reviews the psychological and behavioural effects of online harassment, and proposes criteria for classifying doxxing events as information operations. As a preliminary statement, the deciding factors are target selection, scale and coordination.

As a conceptual study, the paper employs structured synthesis of the previously produced literature with a doctrinal analysis of information operations frameworks as its tool. The paper does not test the propositions empirically. The contribution is the theoretical framework and a classification rubric. All of this is derived from synthesis. The research questions and hypothesis are laying the ground for further empirical work. Even though they are not tested in this paper, they are important stepping stones to secure the digital presence of a nation's military, police and special security services personnel.

7 Douglas 2016.
8 Douglas 2016.
9 Joint Chiefs of Staff 2012.
10 Tucker 2015.
11 Huey et al. 2025.
12 NATO 2023.

Conceptual framework

Doxxing and information operations both operate through the information environment.[13] The information environment is the aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how people derive meaning from information and act on it.[14] Doxxing also bridges online and offline spaces, because it moves personal information into undesired spaces and makes it available to hostile individuals or entities.[15]

Defining information operations and influence operations

Joint doctrine defines information operations as the integrated employment of communication- and information-related capabilities in order to influence, disrupt, corrupt, or usurp the decision-making of adversaries while protecting one's own.[16] The keywords are integrated employment and influence over decision-making.[17] At the same time, it is essential to protect one's own information systems. The target is cognitive, because the cognitive dimension encompasses the minds of those who collect, transmit, receive, respond to, or analyse information.[18] NATO doctrine similarly defines information operations as a function that works with and on information to achieve mission objectives, and as supporting activities focused on convincing, reinforcing, or altering the opinions of adversarial populations in support of objectives.[19]

Psychological operations are always planned and approved. Their goal is to convey previously prepared information in order to influence the emotions, motives, objective reasoning, and behaviour of foreign governments, organisations and individuals.[20] A NATO definition of psychological operations similarly emphasises planned activities directed at approved audiences in order to influence perceptions, attitudes, and behaviour in support of political and military objectives.[21]

Influence operations are not employed by militaries alone. Various cyber actors, nation-state-affiliated advanced persistent threat (APT) groups and hacktivist groups also seek to influence how information is perceived by the public. Social media researchers have observed deliberate activities by cyber threat actors intended to sway public opinion and to manipulate decision-making globally.[22] Examples include the election influence campaigns of recent years in Moldova, Romania and Hungary.[23] Like other military operations, influence operations cannot be executed without

[13] Eckert – Metzger-Riftkin 2020a.
[14] U.S. Department of Defense 2023.
[15] Eckert – Metzger-Riftkin 2020a.
[16] Joint Chiefs of Staff 2014.
[17] National Institute of Standards and Technology s. a.
[18] Joint Chiefs of Staff 2012.
[19] NATO 2023.
[20] Joint Chiefs of Staff 2010.
[21] Avădănei 2022.
[22] Pastor-Galindo et al. 2025.
[23] Harward 2025; Swanson 2018.

being broken down into phases – namely planning, information gathering, execution and assessment.[24]

Definition of doxxing

As a first step, doxxing must be distinguished from accidental information disclosure.[25] Accidental disclosure can occur – among other ways – during a ransomware attack (as in the case of the Hungarian Védelmi Beszerzési Ügynökség [Defence Procurement Agency])[26] or through misconfigured cloud storage (as in the 2023 Pentagon email leak).[27]

Doxxing is frequently defined as the intentional publication of personal information that makes an individual recognisable, with the aim of disclosing, humiliating and threatening.[28] This account explains how doxxing moves personal information from expected, private spaces to undesired surfaces, through which the data becomes available to hostile individuals or entities.[29]

For this paper, doxxing is defined as the non-consensual public dissemination of personally identifying or private information, intended to expose, intimidate, harass, delegitimise, or physically endanger a person.[30] By publishing personal information, the threat actor seeks an audience that may act on it.

Literature review

The literature on doxxing comes mainly from research on online harassment and minority group rights. Case studies, legal analysis, and some conceptual work form the core of most published papers and books, and the literature treats doxxing as technology-facilitated violence and as part of broader harassment processes.[31] This section synthesises definitions, harms, target selection, coordinated campaigning, and effects on behaviour and decision-making, opening the way to treating doxxing as a form of information operation under certain conditions.

[24] Pastor-Galindo et al. 2025.
[25] Anderson–Wood 2021.
[26] The Hungarian Védelmi Beszerzési Ügynökség [Defence Procurement Agency] (VBÜ) is responsible for the procurement of military equipment. In 2024 the organisation was attacked by the INC Ransomware group. Besides stolen procurement-related documents, personal information was also published on the threat actor's dark web page. See Antoniuk 2024.
[27] According to an independent security researcher, the U.S. military's internal emails were accessible for two weeks without authentication. The exposed server leaked approximately three terabytes of U.S. Special Operations Command (USSOCOM) internal emails. See Hope 2023.
[28] Douglas 2016.
[29] Eckert – Metzger-Riftkin 2020a.
[30] Ong 2025.
[31] Eckert – Metzger-Riftkin 2020a.

Typologies of doxxing

Doxxing is described as a serious violation of privacy and security because it involves the unauthorised and often malicious publication of personal or confidential information.[32] It is also described as an attack that can cause substantial harm, ranging from harassing comments to direct physical danger.[33] In the first months of the Russia–Ukraine war, the personal data of around 120,000 Russian soldiers was reportedly published on Telegram channels. Although the recency and accuracy of the data may be questioned, such disclosure could cause irreparable damage to operations.[34] In a 2015 Facebook post, U.S. Central Command stated that the compilation of "death lists" containing service members' data had become the "new norm", and asked personnel and their families to limit their online data sharing.[35] Beyond personal data (names, addresses, telephone numbers, email details, financial information and images), the doxxing of uniformed personnel not infrequently extends to the same data about their loved ones.[36]

Typologies classify doxxing by the mechanism of exposure.[37] One widely used typology distinguishes deanonymisation, targeting and delegitimisation:[38]

- Deanonymising doxxing releases information that reveals the identity of a previously anonymous or pseudonymous person.
- Targeting doxxing reveals information that allows a person to be physically located.
- Delegitimising doxxing releases private information intended to undermine credibility, reputation, or character.[39]

A second typological strand focuses on motivations and uses, identifying extortion, silencing, retribution, control and reputation-building.[40] Process models highlight that doxxing involves a reconnaissance stage, a release stage, and a response stage – the last of which requires an audience that may wish to inflict harm on the identified individual.[41]

Psychological effects

Several articles describe doxxing as capable of causing psychological distress. In harassment and cyberstalking research, victims may suffer high levels of distress. As

[32] Tan 2023.
[33] Snyder et al. 2017.
[34] Jensen–Watts 2022.
[35] U.S. Central Command 2015.
[36] Factually 2026.
[37] Anderson–Wood 2022.
[38] Douglas 2016.
[39] Douglas 2016.
[40] Anderson–Wood 2021.
[41] Bulgakova 2025.

scholars note, this stress is broadly comparable to the symptoms seen in post-traumatic stress disorder.[42]

Harassment research – in studying street harassment – has documented trauma narratives.[43] Victims reported longer-term fear, anxiety and anger. In the worst cases, these feelings outlasted the initial incident, leaving the harassed individuals with the tormenting sense of being constantly about to be attacked.[44] Harassment also damaged self-esteem, with participants describing being made to feel low, dirty, disgusting and degraded.[45]

Doxxing-specific qualitative research likewise supports the experience of acute shock. Participants reported being in an *emergency mode*. This might indicate the state of acute stress in which victims struggle to regain control over their exposed information. Contacting the exposing platforms, warning family members, locking down accounts are all steps taken by victims to mitigate the risk arising from the doxxing event. Despite their effort, they most probably cannot stop its spreading. Even as they tried to regain control over their information once they became aware of the doxxing, they could not.[46]

Behavioural effects

Inciting fear and threatening violence can lead directly to behavioural change. At the beginning of 2026, three Hungarian and one Romanian teenager were arrested after using leaked personal data to threaten attacks on police units. Authorities stated that the incidents formed part of coordinated swatting and doxxing campaigns.[47] Such campaigns are able to cause damage because their aim is not disclosure for its own sake but the intimidation of the targets. Intimidation could incite behavioural change, and behavioural change has been documented in response to online harassment and doxxing exposure.[48] Because journalism research has examined how doxxing produces behavioural change most thoroughly, the effect is illustrated here through that field. In journalism research, self-censorship was used when reporting on certain topics in order to avoid threats and hatred.[49] Other journalism research indicates that online comments influence job satisfaction, focus, self-esteem, frustration and anger. It can lead journalists to avoid certain topics or stories.[50]

It has also been shown that personal accounts (e.g. social media accounts) referenced in doxxing files are more likely to be closed or made private than comparable accounts after the doxxing occurs.[51] This is a clear illustration of behavioural change,

[42] Short et al. 2015.
[43] Thornton et al. 2024.
[44] Thornton et al. 2024.
[45] Thornton et al. 2024.
[46] Eckert – Metzger-Riftkin 2020b.
[47] Antoniuk 2026.
[48] Snyder et al. 2017.
[49] Björkenfeldt 2026.
[50] Carlson–Witt 2020.
[51] Snyder et al. 2017.

as personal data exposure led targets to reduce their visibility and participation in order to avoid further harm.[52]

Target populations

Target selection is extremely important for classifying an event as an information operations manoeuvre. Doxxing perpetrators may target not only the victim but also members of their household, family and circle of friends. This matters for behaviour change because threatening or exposing family members can increase perceived vulnerability.[53]

Studies of the doxxing of police officers illustrate how targeting helps threat actors physically locate a victim. In certain cases, the unauthorised disclosure of a location was accompanied by messages urging followers to harass an individual or his family.[54] In one documented case, online doxxing immediately resulted in a police chat group receiving numerous death threats.[55]

Journalistic pieces and security reportings also describe military and security targets.[56] In 2015, an ISIS-linked group posted the names, photographs, and addresses of U.S. combat pilots and other military personnel.[57] After releasing the information, the group asked its followers to "take the final step".[58]

Coordinated campaigns

Doxxing cannot be described as an act that stands alone. Embedded in a complex influence campaign, it can cause greater damage.[59] Some authors describe doxxing as an offshoot of espionage, reasoning that information obtained through a cyberattack can be disclosed in order to undermine an adversary.[60] In my opinion this perspective offers further reason why doxxing could, and should, be considered an information operation.

Bots have featured in many information operations, mainly influence operations, but they can also be used in doxxing. Coordinated bot groups can attack specific users effectively, frightening the targeted user into silence or driving them off the platform on which they were attacked.[61]

[52] Ong 2025.
[53] Budianto–Hendrayadi 2023.
[54] Huey et al. 2025.
[55] Huey et al. 2025.
[56] Arizanti 2026.
[57] Tucker 2015.
[58] Tucker 2015.
[59] Brangetto–Veenendaal 2016.
[60] Brangetto–Veenendaal 2016.
[61] Woolley 2024.

Research gaps

The reviewed literature describes how doxxing has evolved from a privacy violation into something that can be read as an information operation. No direct link, however, has yet been established. This paper identifies the following research gaps:

- *Conceptual gap.* Doxxing is rarely listed in information operations doctrine. Both U.S. and NATO doctrines stress influencing decision-making and audience behaviour rather than personal data exposure as a distinct method.[62] Yet doxxing is itself capable of intimidating service members, and when used against personnel working in national security it can function as a weapon.[63] Future work should consider doxxing as an act that may affect an adversary's decision-making process.
- *Fragmented definitions.* Definitions of doxxing varies greatly. Some authors highlight the non-consensual publication of private or identifying information.[64] Others stress contextual integrity and the movement of information into *undesired online spaces.*[65] Still others argue that some definitions are too vague, covering almost any disclosure.[66] Closing this gap requires a cross-disciplinary definition narrow enough to serve as a basis for measurement.
- *Limited research on military, police and national security personnel.* As illustrated above, doxxing targets police officers, special agents and military personnel. Future studies should compare doxxing impacts across roles and institutional affiliations, including these groups.[67]
- *Attribution and intent.* Most definitions hold that doxxing is intentional and that its goal is to humiliate, intimidate and punish.[68] Although motivations are usually identified, little research asks whether a given instance is an isolated incident or campaign-integrated.[69] Research should develop attribution grounded in observable features, such as integration with espionage-derived disclosure and connection to other influence operations.[70]

This paper addresses the conceptual gap by aligning the information disclosure mechanism of doxxing with doctrinal definitions that focus on affecting cognition, decision-making, and behaviour through integrated information activities.[71] It narrows definitional ambiguity by adopting an intentional, non-consensual disclosure definition, and it uses typologies that distinguish deanonymising, targeting and delegitimising harms.[72] The article does not resolve attribution and scale questions

[62] Joint Chiefs of Staff 2012; NATO 2023.
[63] Anderson–Wood 2021; Ong 2025.
[64] Douglas 2016; Ong 2025; Tan 2023.
[65] Eckert – Metzger-Riftkin 2020a.
[66] Fang et al. 2023.
[67] Tucker 2015.
[68] Anderson–Wood 2021.
[69] Bulgakova 2025.
[70] Brangetto–Veenendaal 2016; Pastor-Galindo et al. 2025.
[71] Joint Chiefs of Staff 2012; NATO 2023; U.S. Department of Defense 2023.
[72] Anderson–Wood 2021; Douglas 2016.

empirically, but it argues that audience size and attacker coordination are central to downstream effects.[73] My goal is to make the link explicit. Today the existing literature treats doxxing as a privacy harm, while information operation as a strategic capability, I argue that these two meet at a certain point. In my paper I define that point and develop criteria for that.

Research questions and hypotheses

This paper treats doxxing as a potential form of information operation, on the grounds that it can change cognition and behaviour in target audiences. The research questions concern classification and the points at which disclosure can lead to behavioural change.

Research questions

RQ1. When should doxxing be understood as targeting a single individual, and when does it involve a larger community? Answering this question clarifies how such an act can be called an information operation aimed at influencing decision-making in a target population.
RQ2. How can personal data exposure lead to long-term fear, distress and PTSD-like, complex mental states, including withdrawal from public roles?
RQ3. Which behavioural changes signal success from the perspective of an influence campaign?
RQ4. What kinds of coordination, amplification, and persistence make doxxing more likely to function as a campaign rather than a one-off event?

Hypotheses

H1. Doxxing is more likely to qualify as an information operation when it is integrated with other influence techniques.
H2. Doxxing produces behaviour change through psychological distress and perceived vulnerability, because harassment is associated with distress and trauma-like symptoms.
The hypotheses are conceptual propositions, not foreseen to produce empirical results. Future research must follow to operationalise the hypotheses.

Theoretical argument

To argue that doxxing belongs to the sphere of information operations, one must accept that the claim is conditional – doxxing is not always an information operation.

[73] Wang et al. 2025.

Some doxxing events can be functionally equivalent to information operations when they are planned information activities designed to create cognitive effects. To examine H1, this paper draws on doctrinal definitions of information and psychological operations, as well as on doxxing typologies and the motives behind doxxing (notably coercion and targeting).

Functional equivalence

I argue that doxxing can be equated with information operation in case doxxing fulfils the following three criteria:

- role-bearing target
- an intent to shape behaviour
- dissemination of information to mobilise the receivers of the information

Information operations target an audience's situational assessment, intentions and capabilities – not only for military purposes but also in political, civilian and hybrid environments.[74] Achieving the intended effect therefore requires accurately identifying the audience and selecting the message and the means by which the operation is conducted. The audience must comply with, identify with, or internalise the message for the objective – or to say it more simply, influence the decision-making process.[75] This feature aligns with the information operations focus on affecting cognition and decision-making by shaping perceived risks through information disclosure and audience mobilisation.[76] The terms information operation and doxxing should be treated as equated on certain terms. In the doctrinal definition of information operation influence, disruption and altering of the decision-making process appear. These effects can be found in doxxing as well. Because of their shared mechanism and effect, I treat equivalence not as a metaphor but as a claim.

NATO information operations doctrine likewise defines such planned activities as supporting manoeuvres to influence behaviour, attitudes and perception. When doxxing is planned and integrated into a campaign, it can be seen as an information-related technique used to create desired cognitive and behavioural effects.[77]

Mechanisms of behaviour change

The three dimensions of information operations are the cognitive, the physical and the informational, representing the human, material, and technological domains in which influence effects are applied.[78]

[74] Haig 2022.
[75] Joint Chiefs of Staff 2014.
[76] Bulgakova 2025; Joint Chiefs of Staff 2012.
[77] Brangetto–Veenendaal 2016.
[78] Haig 2022.

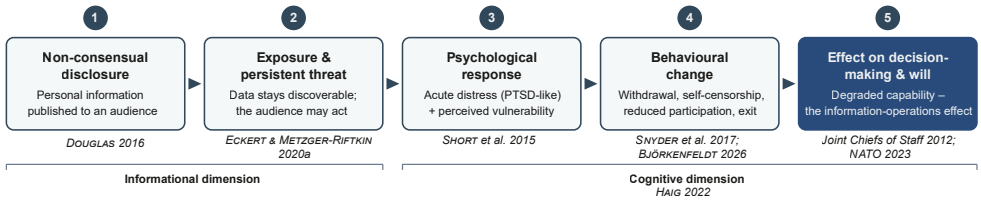


Figure 1: The doxxing-to-behaviour mechanism
Source: compiled by the author

The mechanisms of doxxing are partly informational and partly cognitive. They are informational because publishing unwanted information online disrupts privacy. Once personal information is shared on an open platform, the victim may fear physical harm in the real world.[79] Because at present there is no reliable means of removing information from the internet, doxxing information may remain discoverable indefinitely.

Distress follows directly from unwanted information exposure. According to the literature, it can resemble PTSD symptoms, which are described as interfering with occupational activity and social relations, and the affected person may withdraw from public engagement (see Figure 1).[80]

Journalists have described fear for their personal safety and hesitation before covering controversial topics or posting certain information online, indicating a direct link to behavioural restraint.[81]

Boundary cases and counterarguments

A classification framework must separate doxxing from legitimate information publishing, such as whistleblowing, where disclosure occurs in the public interest rather than out of ill will.[82] Because doxxing definitions are sometimes overly broad and cover almost any disclosure, the framework must clearly specify who may legitimately be subject to public scrutiny through disclosed information. Such guidance belongs to research and policy classification.[83]

A second boundary concerns intent and effect. Unintentional or accidental publication occurs (e.g. an email containing personal data sent to the wrong address, or a lost storage device holding personal data). Doctrine emphasises that information operations must be integrated and orchestrated within a previously approved plan, which implies that isolated doxxing cannot be called an information operation.[84]

[79] Ong 2025.
[80] Short et al. 2015.
[81] Carlson–Witt 2020.
[82] Fang et al. 2023.
[83] Fang et al. 2023.
[84] Joint Chiefs of Staff 2012.

Finally, not all doxxing aims to achieve behaviour change in the target. Yet even without that intention, a threatening audience may form and seek to harass the doxxed person.[85]

Criteria

Merging information operations doctrine with the doxxing literature calls for a multi-criteria approach. The doctrine focuses on integration, targeting, cognitive effects and behavioural change as the final step.[86] The doxxing literature focuses on intentional information release, the inducement of fear and audience response.[87]

Intent

Intent is central to the definitions of both doxxing and information operations. Doxxing is defined as the intentional public release of personal information, often intended to intimidate or punish. Information operations are defined as deliberate activities aimed at influencing decision-making to achieve objectives. Where an intent to influence the public or decision-making bodies can be identified in the motives behind doxxing, the event can be said to constitute an information operation.

Target

Choosing the target is an essential part of both doxxing and information operations. Doxxing is more likely to constitute a form of information operation when it is directed at organisational roles (e.g. police officers, military personnel). Such targets are chosen in order to pressure behaviour change.[88]

Scale

Scale – the size of the audience – is relevant because doxxing is intended to reach many people.[89] Because information posted online may remain available indefinitely, scale increases exposure and the probability of further audience action over time.[90] Scale can also confer an operational advantage – a large target population, such as a doxxing list of many military personnel, can heighten collective fear.[91]

[85] Flewelling 2023.
[86] Joint Chiefs of Staff 2012; NATO 2023.
[87] Anderson–Wood 2021; Eckert – Metzger-Riftkin 2020a.
[88] Huey et al. 2025; Tucker 2015.
[89] Ong 2025.
[90] Eckert – Metzger-Riftkin 2020a.
[91] Huey et al. 2025; Tucker 2015.

Coordination

Coordination is a key element of information operations doctrine, requiring planning, integration, and thorough orchestration to achieve the set goals.[92] Influence operations frameworks use techniques such as amplification and the flooding of the information space.[93] As shown in earlier examples, doxxing can be integrated into influence operations. Moreover, gathering information for doxxing requires reconnaissance and can be seen as an offshoot of espionage, in which stolen information is disclosed to undermine an adversary.[94] Doxxing can therefore be listed among information operations techniques when it is coordinated with other campaign elements.

Behavioural effect

Information operations doctrine holds that information activities aim to alter behaviour.[95] Doxxing is defined as an intimidating act achieved through the non-consensual publication of personal information.[96] Empirical work shows that withdrawal behaviour follows such acts – including account closure, increased privacy settings, self-censorship, or the avoidance of certain topics.[97] A doxxing event can be listed among information operations where there is observable change in the target's organisational engagement, participation, or speech.[98]

Scoring rubric

The rubric in Table 1 summarises the criteria for classifying a doxxing episode as an information operations candidate.[99] It is designed for research coding and structured case comparison rather than for legal adjudication. A simple additive scoring function is used, $S = \Sigma\, s_i$ for $i = 1$ to 5, where each criterion is scored from 0 to 3, giving a maximum of 15. Higher scores indicate stronger functional similarity to information operations doctrine and influence campaign logic.

A classification threshold of $S \geq 11$ is proposed for an *information operations candidate,* because this level requires several criteria to be at least moderate rather than allowing qualification on intent or individual harm alone. Consistent with Section *Boundary cases and counterarguments,* coordination has a special status. Because doctrine treats integration as constitutive of an information operation, a score of 0 on Coordination is a strong contraindication even where other criteria score highly. Both the threshold and this qualification are proposed heuristics for research use and require empirical calibration.

[92] Joint Chiefs of Staff 2012.
[93] Pastor-Galindo et al. 2025.
[94] Brangetto–Veenendaal 2016.
[95] NATO 2023.
[96] Ong 2025.
[97] Björkenfeldt 2026; Snyder et al. 2017; Wang et al. 2025.
[98] Huey et al. 2025; Wang et al. 2025.
[99] NATO 2023.

Table 1: Scoring rubric for classifying a doxxing episode as an information operations candidate

Criterion	0 score	1 score	2 score	3 score
Intent	No evidence of intent to influence beyond interpersonal harm[100]	Intent to punish or shame a target[101]	Intent to intimidate or silence a target, or to enact revenge, as reported by targets or described by perpetrators[102]	Intent linked to objectives to influence decision-making or participation, consistent with influence and information operations logic[103]
Target	Target is not linked to institutional roles or collective decision nodes[104]	Target is an individual without clear organisational relevance, though exposure creates a risk of harassment[105]	Target is a role-bearing individual (journalist, activist, officer) with a public-facing function, with explicit intimidation or targeting to enable physical location[106]	Target set is an organisational choke-point population (e.g. officers policing protests, military personnel lists), with an explicit logic of raising costs so that members refrain from serving[107]
Scale	Limited dissemination and minimal evidence of audience response[108]	Public release occurs, but audience mobilisation is unclear[109]	Release is publicised to create an audience that may act, consistent with a response stage requiring an audience[110]	High-volume audience attack or list-style targeting that plausibly increases behavioural change[111]
Coordination	No evidence of planning or integration with other actions[112]	Some sequencing or staging (reconnaissance–release–response) without broader campaign context[113]	Evidence of phased planning or integration with other influence techniques[114]	Evidence of integration into a wider influence operation or espionage-derived disclosure[115]
Behavioural effect	No detectable change in behaviour, participation, or expression[116]	Individual-level withdrawal, such as making accounts private or closed[117]	Withdrawal from public appearances or self-censorship to avoid threats and hatred[118]	Organisational or role-level behaviour change, such as reduced volunteering, ingrained self-censorship, or delayed posting under sustained attack[119]

Source: compiled by the author

[100] Tan 2023.
[101] Flewelling 2023.
[102] Eckert – Metzger-Riftkin 2020b; Ong 2025.
[103] Joint Chiefs of Staff 2012; Pastor-Galindo et al. 2025.
[104] Anderson–Wood 2021.
[105] Snyder et al. 2017.
[106] Douglas 2016; Huey et al. 2025.
[107] Huey et al. 2025; Tucker 2015.
[108] Anderson–Wood 2021.
[109] Snyder et al. 2017.
[110] Bulgakova 2025; Ong 2025.
[111] Tucker 2015; Wang et al. 2025.
[112] Fang et al. 2023.
[113] Bulgakova 2025; Ong 2025.
[114] Pastor-Galindo et al. 2025.
[115] Arizanti 2026; Brangetto–Veenendaal 2016.
[116] Fang et al. 2023.
[117] Snyder et al. 2017.
[118] Björkenfeldt 2026; Carlson–Witt 2020.
[119] Björkenfeldt 2026; Wang et al. 2025.

Application to cases

I applied the above detailed scoring rubric to three cases. Two cases were described earlier, while one boundary case is brought in to test. The scores are based on my analytical judgement and the reported claims should be read with the caveats in Section *Limitations*.

Case 1. The Islamic State's "hit list" of U.S. military personnel[120]

I score Intent at 3 because the group not only disclosed the information but urged its followers to harm the soldiers. The threat was not against a single person but against the military community. Target is also 3. The released names were those of combat pilots. Specially trained, hard to substitute population. The Scale is also 3. ISIS disclosed a list to a population which was known to be aggressive towards U.S. military personnel. Coordination is on 2. This is so, because even though the release of the information was carried out in an organised way, it has not been proved to be part of a wider propaganda effort. The Behavioural effect is also 2. The U.S. Central Command issued a public advisory. However, direct measurements of withdrawal from online engagement are not tracked. The total point is 13, therefore this event classifies as an information operation candidate.

Doxxing police officers during protest duties[121]

I score Intent as 3 because the disclosures were aimed at deterring police officers from taking on protest policing duties. Target is 3, since the officers who assigned to control protesters were a special group at that time in the police force. Scale is 2. The published information was not evenly distributed, even though it sometimes called for violence. Coordination is 2 since this event is not directly related to broader information operation. However, it had a strong aim to disturb protest policing forces. Behavioural effect is 3. The role-based pressure achieved its goal – numerous police officers retained from serving on such duty. The total is 13, so this event qualifies as information operation as well.

Disclosure of a former partner's address as a revenge (boundary case)

Intent is 1, because the aim is not to influence the general population, but to punish a single person. Target is 0, since the doxxed person is not important in the collective decision-making, nor does he/she hold an important function. Scale is 1. Despite the fact that the information is published, there is no or low audience mobilisation.

[120] Tucker 2015.
[121] Huey et al. 2025.

Coordination is 0. Since the action was not prepared for staging, integration in other actions, this category can be dismissed. The Behavioural effect can be set at 3, since the victim will most probably withdraw. Population-level effect is non-existent in this case. The total is 5.

Table 2: Illustrative application of the rubric to three cases

Case	Intent	Target	Scale	Coordination	Behaviour	Total	Result
1. IS military "hit list"	3	3	3	2	2	13	IO candidate
2. Protest-policing doxxing	3	3	2	2	3	13	IO candidate
3. Private revenge doxxing	1	0	1	0	3	5	Private abuse

Note: Criteria are scored 0–3. The maximum is 15 and the classification threshold is S ≥ 11. Scores are the author's analytical judgements applied to the published record. Figures in the security cases are reported claims.
Source: compiled by the author

Discussion

The literature supports listing doxxing among information operations, because doxxing can serve as a planned information activity that targets cognition and behaviour through intimidation, delegitimisation and audience mobilisation.[122] This is consistent with the information operations doctrines, which hold that the ultimate target of an information operation is the human decision-making process, and with influence operations frameworks that include harassment and target degradation to discredit, intimidate, or silence challengers to a narrative.[123] Placing it together, it can be stated that the observations are not of a mere surface resemblance. The doctrinal definitions and the doxxing evidence describe the same sequence. It looks as the following: information is disclosed and the target's behaviour changes in a way that the discloser planned. While this happens, an audience is mobilised. Based on these observations, I treat the two bodies of work as describing one phenomenon from two vantage points. Doxxing does not just resemble information operation but it is an example of that whenever the set conditions are met.

Doxxing used against police officers during protests, intended to raise the costs of participation, exemplifies an explicit behaviour change objective.[124] The mobilising and intimidating effect of doxxing is also illustrated by the threatening telephone calls received by doxxed military personnel.[125] If I examine the patterns across these cases, it will be revealed that actors as different as protest groups, state-linked threat actors or jihadi groups arrived at the same technique. All of them recognised that

[122] Bulgakova 2025; Douglas 2016; NATO 2023.
[123] Pastor-Galindo et al. 2025.
[124] Huey et al. 2025.
[125] Tucker 2015.

publishing the personal data of role-bearing personnel will produce the same result. This convergence matters, because it proves that the deterring effect of doxxing is reproducible and is understood by those who engage in it. A single act of information disclosure most probably will not change the population's behaviour. However, targeted disclosure aimed at the professional community can. From the previously described examples it is clear that threat actors are aware of it.

The literature on coordinated campaigns further supports listing doxxing among influence operations. By shaming and embarrassing the victim, doxxing – like other influence operations – undermines an adversary through the disclosure of information.[126] This reframes where the harm of operational doxxing actually is. The named individual is only a tool in this operation. The intended target is the audience that watches – which can be the fellow servicemen or the general public. The goal of the threat actor is to deter others of taking on the responsibilities and to discredit the unit or the whole service. In one sentence: the individual is harmed while the audience is influenced.

Limitations

Several limitations qualify this argument. Direct empirical evidence that doxxing causes behaviour change is limited, as demonstrated in this paper, and much of the psychological evidence is drawn from harassment and cyberstalking samples rather than from doxxing-only studies.[127] In addition, the proposed rubric is not empirically validated, and the $S \geq 11$ threshold is a reasoned heuristic that requires calibration against coded cases. The doctrinal focus is also primarily Western (U.S. and NATO), and other doctrinal traditions might conceptualise information confrontation differently.

Conclusion

Doxxing is the intentional, non-consensual publication of personal information online, often with the aim of humiliating, intimidating, threatening, or punishing. It can enable real-world harassment and physical danger. Information operations are the integrated employment of information-related capabilities to influence or disrupt decision-making.[128] The literature shows that harassment can generate distress resembling PTSD, which can interfere with occupational and social functioning,[129] and that doxxing produces behavioural and withdrawal effects, such as withdrawal behaviour and the avoidance of contacts and topics.[130]

Together, these bodies of evidence support a structured argument that doxxing can be listed among information operations under specified conditions. Doxxing can be classified as an information operation when:

[126] Brangetto–Veenendaal 2016.
[127] Ong 2025; Short et al. 2015.
[128] Joint Chiefs of Staff 2012; NATO 2023.
[129] Short et al. 2015.
[130] Björkenfeldt 2026; Snyder et al. 2017; Wang et al. 2025.

- it is planned and coordinated
- it targets role-bearing persons or key figures
- it mobilises an audience to act
- it produces observable behavioural change aligned with an objective

If doxxing is treated as a privacy violation, it will be on the table of data protection officers. However, if it is treated as an information operation, it will be an urgent topic for force protection and institutional resilience. I argue that scholars studying security should accept the second register.

References

Anderson, Briony – Wood, Mark A. (2021): Doxxing: A Scoping Review and Typology. In Bailey, Jane – Flynn, Asher – Henry, Nicola (eds.): *The Emerald International Handbook of Technology-Facilitated Violence and Abuse.* Leeds: Emerald Publishing, 205–226. Online: https://doi.org/10.1108/978-1-83982-848-520211015

Anderson, Briony – Wood, Mark A. (2022): Harm Imbrication and Virtualised Violence: Reconceptualising the Harms of Doxxing. *International Journal for Crime, Justice and Social Democracy,* 11(1), 196–209. Online: https://doi.org/10.5204/ijcjsd.2140

Antoniuk, Daryna (2024): Hungary Confirms Hack of Defense Procurement Agency. *The Record,* 14 November 2024. Online: https://therecord.media/hungary-defense-procurement-agency-hacked

Antoniuk, Daryna (2026): Teen Swatting Suspects Arrested in Hungary and Romania. *The Record,* 28 January 2026. Online: https://therecord.media/teen-swatting-doxxing-suspects-arrested-hungary-romania

Arizanti, Michael (2026): Doxxing of India's Top Military Officer Reflects a New China–Pakistan Tactic. *The Times of Israel,* 14 May 2026. Online: https://blogs.timesofisrael.com/doxxing-of-indias-top-military-officer-reflects-a-new-china-pakistan-tactic/

Avădănei, Angela-Karina (2022): Influence Operations, between the Ethical and Critical Facet. *Romanian Military Thinking,* (3), 74–87. Online: https://doi.org/10.55535/RMT.2022.3.05

Björkenfeldt, Oscar (2026): Self-Censorship in Journalism: The Role of Emotional, Professional, and Institutional Factors. *Digital Journalism,* 14(3), 493–510. Online: https://doi.org/10.1080/21670811.2025.2601961

Boda, Mihály (2018): Az alapvető katonai erények mibenléte és helyük a hosszú 19. századi magyar hadtudományos gondolkodásban: 3. rész – A becsület. *Hadtudomány,* 28(3–4), 17–30. Online: https://doi.org/10.17047/HADTUD.2018.28.3-4.17

Brangetto, Pascal – Veenendaal, Matthijs A. (2016): Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. In *2016 8th International Conference on Cyber Conflict (CyCon),* 113–126. Online: https://doi.org/10.1109/CYCON.2016.7529430

Budianto, Azis – Hendrayadi, Agus (2023): Juridical Review of the Criminal Act of Doxing: Dissemination of Personal Data without Permission in the Perspective of Law No. 19 of 2016 Concerning EIT. In *Proceedings of the 3rd Multidisciplinary International Conference (MIC 2023).* Online: https://doi.org/10.4108/eai.28-10-2023.2341796

Bulgakova, Daria (2025): Doxing: The Sandy Hook Case Study. *NaUKMA Research Papers. Law,* 14, 3–18. Online: https://doi.org/10.18523/2617-2607.2024.14.3-18

Carlson, Caitlin R. – Witt, Haley (2020): Online Harassment of U.S. Women Journalists and Its Impact on Press Freedom. *First Monday,* 25(11). Online: https://doi.org/10.5210/fm.v25i11.11071

Douglas, David M. (2016): Doxing: A Conceptual Analysis. *Ethics and Information Technology,* 18(3), 199–210. Online: https://doi.org/10.1007/s10676-016-9406-0

Eckert, Stine – Metzger-Riftkin, Jade (2020a): Doxxing. In Ross, Karen – Bachmann, Ingrid – Cardo, Valentina – Moorti, Sujata – Scarcelli, Cosimo M. (eds.): *The International Encyclopedia of Gender, Media, and Communication.* Hoboken: Wiley Blackwell – ICA, 1–5. Online: https://doi.org/10.1002/9781119429128.iegmc009

Eckert, Stine – Metzger-Riftkin, Jade (2020b): Doxxing, Privacy and Gendered Harassment: The Shock and Normalization of Veillance Cultures. *Medien & Kommunikationswissenschaft,* 68(3), 273–287. Online: https://doi.org/10.5771/1615-634X-2020-3-273

Factually (2026): Have ICE Agents or Their Families Been Doxxed? *Factually,* 27 January 2026. Online: https://factually.co/fact-checks/politics/have-ice-agents-or-families-been-doxxed-23887e

Fang, Yuan – Risius, Marten – Cheung, Christy (2023): Understanding the Current State of Knowledge and Future Directions of Doxing Research: A Social Cognitive Theory Perspective. In *Proceedings of the 56th Hawaii International Conference on System Sciences.* Online: https://doi.org/10.24251/HICSS.2023.672

Flewelling, Riley (2023): Not Just Words: Grappling with the Doxing of Civilians in War. *Center on Law, Ethics and National Security, Essay Series,* (19). Online: https://sites.duke.edu/lawfire/files/2023/07/R.-Flewelling-Essay-7.25.23.pdf

Haig, Zsolt (2022): Kibertéri kognitív befolyásolás az információs műveletekben. *Hadtudományi Szemle,* 15(2), 115–130. Online: https://doi.org/10.32563/hsz.2022.2.7

Harward, Christina (2025): Russia Continues Efforts to Regain Influence over Moldova. *Institute for the Study of War,* 5 September 2025. Online: https://understandingwar.org/research/russia-ukraine/russia-continues-efforts-to-regain-influence-over-moldova/

Hope, Alicia (2023): The Pentagon Leaked Sensitive Military Emails via a Misconfigured Microsoft Azure Government Cloud. *CPO Magazine,* 2 March 2023. Online: www.cpomagazine.com/cyber-security/the-pentagon-leaked-sensitive-military-emails-via-a-misconfigured-microsoft-azure-government-cloud/

Huey, Laura – Ferguson, Lorna – Towns, Zachary (2025): „Cops Need Doxxed": Releasing Personal Information of Police Officers as a Tool of Political Harassment. *Crime & Delinquency,* 71(3), 714–739. Online: https://doi.org/10.1177/00111287241271069

Jensen, Eric – Watts, Sean (2022): Ukraine Symposium – Doxing Enemy Soldiers and the Law of War. *Lieber Institute West Point,* 31 October 2022. Online: https://lieber.westpoint.edu/doxing-enemy-soldiers-law-of-war/

Joint Chiefs of Staff (2010): *Joint Publication 3-13.2. Military Information Support Operations.* Online: https://info.publicintelligence.net/JCS-MISO.pdf

Joint Chiefs of Staff (2012): *Joint Publication 3-13. Information Operations.* Online: https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf

Joint Chiefs of Staff (2014): *Chairman of the Joint Chiefs of Staff Instruction 3210.01. Joint Information Operations Proponent.* Online: www.jcs.mil/Portals/36/Documents/Library/Instructions/3210_01.pdf

Kovács, László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148(5), 3–18. Online: https://doi.org/10.35926/HSZ.2020.5.1

National Institute of Standards and Technology (s. a.): Information Operations (IO). *Computer Security Resource Center.* Online: https://csrc.nist.gov/glossary/term/information_operations

NATO (2023): *Allied Joint Publication 10.1. Allied Joint Doctrine for Information Operations.* North Atlantic Treaty Organization.

Novak, Matt (2026): How the Definition of "Doxxing" Is Being Twisted into a Weapon of Anonymity. *Gizmodo,* 14 January 2026. Online: https://gizmodo.com/how-the-definition-of-doxxing-is-being-twisted-into-a-weapon-of-anonymity-2000709404

Ong, Rebecca (2025): Hong Kong's Response to the Fight against Doxxing. *Common Law World Review,* 54(1), 17–42. Online: https://doi.org/10.1177/14737795241267290

Pastor-Galindo, Javier – Nespoli, Pantaleone – Ruipérez-Valiente, José A. – Camacho, David (2025): Influence Operations in Social Networks. *arXiv*. Online: https://doi.org/10.48550/ARXIV.2502.11827

Putman, Joanna (2026): "ICE List" Doxxing Site Alleges DHS Whistleblower Leaked Identities of 4,500 Agents. *Police 1,* 14 January 2026. Online: https://globalordnancenews.com/2026/01/14/ice-list-doxxing-site-alleges-dhs-whistleblower-leaked-identities-of-4500-agents/

Short, Emma – Guppy, Andrew – Hart, Jacqui A. – Barnes, James (2015): The Impact of Cyberstalking. *Studies in Media and Communication,* 3(2), 23–37. Online: https://doi.org/10.11114/smc.v3i2.970

Snyder, Peter – Doerfler, Periwinkle – Kanich, Chris – McCoy, Damon (2017): Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing. In *Proceedings of the 2017 Internet Measurement Conference,* 432–444. Online: https://doi.org/10.1145/3131365.3131385

Swanson, Robert C. R. (2018): Two Case Studies of Russian Propaganda in Romania and Hungary. *The International Affairs Review,* 15 February 2018. Online: www.iar-gwu.org/print-archive/64g7lshepy1awksgtiyvj3bsqfipw0

Tan, Albert (2023): *To Dox or Not to Dox, That Is the Question.* Online: www.researchgate.net/publication/368851607_To_Dox_or_Not_to_Dox_that_is_The_Question

Thornton, Georgina – Willmott, Dominic – Richardson, Emma – Hudspith, Lara (2024): Examining the Immediate and Enduring Psychological Impact of Street Harassment on Women's Mental Health. *Mental Health and Social Inclusion,* 28(5), 734–744. Online: https://doi.org/10.1108/MHSI-07-2023-0080

Tucker, Patrick (2015): War by Doxxing. *Defense One,* 23 March 2015. Online: www.defenseone.com/technology/2015/03/war-doxxing/108238/

U.S. Central Command (2015): Message to Service Members Regarding Online Security. *Facebook,* 2015. Online: www.facebook.com/CENTCOM/posts/10153676790449606/

U.S. Department of Defense (2023): *Strategy for Operations in the Information Environment.* Online: https://govwhitepapers.com/whitepapers/strategy-for-operations-in-the-information-environment

U.S. Department of Homeland Security (2025): Anarchists and Rioters in Portland Illegally Dox ICE Officers and Federal Law Enforcement. *U.S. Department of Homeland Security,* 11 July 2025. Online: www.dhs.gov/news/2025/07/11/anarchists-and-rioters-portland-illegally-dox-ice-officers-and-federal-law

Wang, Yian – Umashankar, Mukhilshankar – Chandrasekharan, Eshwar – Sundaram, Hari (2025): The Chilling: Identifying Strategic Antisocial Behavior Online and Examining the Impact on Journalists. *Proceedings of the ACM on Human-Computer Interaction,* 9(7), 1–67. Online: https://doi.org/10.1145/3757668

Woolley, Samuel C. (2024): Propaganda Digital: El poder de las/los influencers [Digital Propaganda: The Power of Influencers]. *Revista Elecciones,* 23(28), 15–40. Online: https://doi.org/10.53557/Elecciones.2024.v23n28.01