European Journal of International Security (2025), page 1 of 19
doi:10.1017/eis.2025.10016

EJIS

RESEARCH ARTICLE

Finding the thieves amongst the liars: Thinking clearly about cyber-enabled influence operations

Christopher Whyte[1] and Ugochukwu Etudo[2]

[1]Homeland Security & Emergency Preparedness, L. Douglas Wilder School of Government & Public Affairs, Virginia Commonwealth University, Richmond, VA, USA and [2]Information Systems, School of Business, Virginia Commonwealth University, Richmond, VA, USA
Corresponding author: Christopher Whyte; Email: cewhyte@vcu.edu

(Received 11 April 2024; revised 4 June 2025; accepted 18 June 2025)

Abstract

How do cyber attacks aid attempts to generate influence? This article argues that cyber-enabled influence operations (CEIO) are more varied in form than is often recognised by scholars. We describe four kinds of CEIO activities – preparatory attacks, manipulative attacks, attacks in parallel, and influence-enabling – and observe that the type most often referenced by scholars (manipulative attacks) is the one whose utility is most substantially constrained by the clashing logics of cyber and influence operations. Our analysis suggests a clear theoretical basis for understanding cyber-influence interactions, namely that the style of cyber operational targeting is inversely tied to the scale of influence outcomes intended by an attacker. Tactics and the conditions that motivate them change as the scale of interference intended by the attacker varies over time, with tools and approaches that offer utility in one phase failing to do so in another as the environment transforms and interacts with attacker interests.

Keywords: cross-domain operations; cyber conflict; cyber operations; hybrid warfare; influence operations; information warfare; subversion

Cyber-enabled influence operations (CEIO) sit at the intersection of two distinct yet increasingly intertwined strategies of statecraft: cyber operations and influence campaigns (a term often used interchangeably with influence operations or IO).[1] While both leverage the internet's global reach, their logics of use differ significantly. Cyber operations typically emphasise secrecy, system compromise, and disruption, while IO focus on manipulating information environments to achieve psychological or socio-political effects. Yet, as states increasingly integrate these approaches, the resulting CEIO remain under-theorised, often conflated, or oversimplified in scholarship.

This conflation has led to significant analytical gaps. The operational dynamics of CEIO – how cyber capabilities augment influence campaigns or vice versa – are poorly understood. For instance, are cyber intrusions primarily preparatory tools, or do they directly create influence effects? What

[1] Throughout this paper, we reference a range of terms, including 'cyber operations', 'influence operations', and 'influence campaigns'. We retain the diverse use of these terms so that readers coming from different theoretical and empirical perspectives can read into their use in the context of specific passages. However, in our analyses, these terms should generally be thought of as distinguishable based on their implied intent and operational focus. Specifically, this article adopts the assumption that terms incorporating the 'cyber' moniker (e.g. 'cyber operations' or 'cyber effects') generally denote actions aimed at achieving effects through technical manipulation of digital systems, such as IT infrastructure or networks. In contrast, terms like 'influence operations' or 'information operations' emphasise psychological or socio-political effects, often targeting human cognition or societal structures. This distinction reflects an effort to disentangle the conflation often seen in literature, recognising that while these domains intersect, their underlying mechanisms and intended outcomes are conceptually distinct.

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

strategic risks and opportunities arise when these domains converge? Addressing such questions is critical to unpacking how CEIO shape modern conflict, particularly as adversaries exploit the digital domain to target democracies.

This article contributes to this growing focus on CEIO by adding clarity on the types of activities that sit at the intersection of these distinct areas of strategic approach and presenting subsequent analytic conclusions. We argue that CEIO are more varied in their form than is often recognised in Security Studies scholarship. This point is significant due to the interaction of different logics of approach to the deployment of the distinct capabilities involved. In addressing questions of state targeting, cross-domain utility, and more, scholars must effectively differentiate between operations that seek to leverage one established logic of interstate engagement to aid another versus more targeted deployment of capabilities to enhance another in isolation.

Specifically, we describe four kinds of cyber-enabled influence activities – (1) *preparatory attacks*, (2) *manipulative attacks*, (3) *attacks in parallel*, and (4) *influence-enabling activities*. Preparatory attacks involve those activities that leverage the intelligence potential of cyber attacks to enhance the potential of a subsequent influence campaign, primarily via actions like reconnaissance, resource generation (e.g. botnet creation), or account takeover but also directed capacity denial or targeted socio-political compromise. Manipulative attacks are the category of activity most commonly discussed by researchers interested in CEIO, constituted of attacks that are intended to create influence in themselves (e.g. by compromising voter systems or poisoning social media algorithms). Attacks in parallel involve cyber activities leveraged against a nation that are contemporaneous with influence activities without clear operational coordination. Finally, influence-enabling attacks reverse the conventional logic of CEIO and see interference activities leveraged to augment the socio-political impact of cyber operations.

An examination of the strategic and operational underpinnings of these categories of CEIO suggests that the type of CEIO most often referenced by scholars – manipulative attacks – is the one whose utility is most substantially constrained by the competing logics of cyber and influence operations. The 'outsider looking in' dynamic of malign foreign influence campaigns produces a series of operational incentives and risks surrounding the use of tactics that overtly disrupt a target national system.[2] As such, cyber attacks that attempt to aid a broader influence campaign via direct attack on national information or socio-political systems risk poisoning the strategic manoeuvre writ large.[3] By contrast, both preparatory activities and attacks in parallel suggest clear additive value for an attacker. However, here also there are operational nuances generated by the underlying character of digital influence activities and projected onto cyber operations decision-making. Preparatory activities, much like manipulative attacks, must toe the line between enhancing an influence operation and risking its credibility, viability, or strategic relevance. Attacks in parallel, by contrast, only augment the impact of influence campaigns sufficient to produce signalling advantages where domestic conditions prime target actors to see linkages beyond the normal background noise that is interstate cyber engagement. This dynamic also impacts the utility of influence-enabling activities, for which operational prospects are inherently limited not only by domestic conditions but also by capacity-building and coordination challenges for the adversary.

Ultimately, this article represents a 'third way' of looking at CEIO between the conflation and the granular tactical questioning that is common in the limited work on the subject in Strategic Studies and related scholarship.[4] Conventionally, such work either blurs the line between cyber and IO (thus creating various terminological issues that are common in the field) or more narrowly

[2] Christopher Whyte and Ugochukwu Etudo, 'Cyber by a different logic: Using an information warfare kill chain to understand cyber-enabled influence operations', in Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec (eds), *Information Warfare in the Age of Cyber Conflict* (Routledge, 2020), pp. 114–31.

[3] Christopher Whyte, 'Beyond tit-for-tat in cyberspace: Political warfare and lateral sources of escalation online', *European Journal of International Security*, 5:2 (2020), pp. 195–214.

[4] Jelena Vićić and Erik Gartzke, 'Cyber-enabled influence operations as a "center of gravity" in cyberconflict: The example of Russian foreign interference in the 2016 US federal election', *Journal of Peace Research* 61:1 (2024), pp. 10–27.

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

attempts to answer questions about the targeting of IO and the pursuant implications for cyber activity. This second focus is a recent turn towards empirical investigation and is extremely welcome. Nevertheless, CEIO work remains limited by the conflation of assumptions about the operational logics and strategic utility of IO and cyber operations. We argue that analytic separation of cyber and influence effect operations is critical to understanding their confluence.

More specifically, our analysis here suggests that understanding CEIO requires recognising their dual dependency on the distinct logics of cyber and influence operations. Specifically, the scale of influence outcomes intended by an attacker often inversely correlates with the intensity and directness of cyber targeting. Tactics and the conditions that motivate them change as the scale of interference intended by the attacker varies over time, with tools and approaches that offer utility in one phase failing to do so in another as the environment transforms (e.g. with a shift in defender awareness or public opinion, the success or failure of other adjunct operations, etc.) and interacts with attacker interests. This insight reframes how we analyse CEIO, emphasising the need to separate these operations' effects and utility analytically in order to strengthen prediction and prevention regimes.

CEIO as a new epicentre for low-intensity conflict

In recent years, the Strategic Studies field has played host to developing debates over how states reap strategic benefits from the deployment of cyber and influence operations (IO).[5] Though interstate activity on both fronts is overtly defined by the internet and its integration with global society, cyber conflict and influence campaigns are argued to retain different logics of use that produce distinct state approaches to operational targeting, capacity building, and more.[6] Ongoing debate among cyber scholars is divided among those who argue that global cyber conflict reflects a form of intelligence contest and those who see the potential for states to use cumulative operations to create conventional strategic advantage.[7] Recent work on IO sees similar division, albeit not yet so clearly defined in theory, between those who see simple opportunity for states to unbalance adversaries and those who see these campaigns as having the potential to help secure strategic objectives via a logic of subversion.[8]

Perhaps the most interesting development concerning both phenomena is the recent scholarly focus on cyber-enabled influence operations (hereafter CEIO),[9] or those instances where cyber mechanisms are deployed in aid of influence campaign objectives (or vice versa). Despite a strong tendency in established scholarship to refer to cyber and influence operations in the same breath, recent work is different. It attempts to not simply conflate the two as similar emergent types of state capacity.[10] Rather, it attempts to problematise and theorise the interaction of these capacities in the context of expanding Western experiences with relevant incidence of cyber-enabled influence. To that point, several expert resources suggest a growing landscape of cases of cyber-enabled influence operations since the mid-2010s, as well as a proliferation of malign actors responsible for such interference.[11]

[5] For the key texts, see among others Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford University Press, 2022); Michael P. Fischerkeller and Richard J. Harknett, 'Deterrence is not a credible strategy for cyberspace', *Orbis*, 61:3 (2017), pp. 381–93; and Amy Zegart, Joshua Rovner, Michael Warner, et al. *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest* (Georgetown University Press, 2023).

[6] Whyte and Etudo, 'Cyber by a different logic'.

[7] Lennart Maschmeyer, 'A new and better quiet option? Strategies of subversion and cyber conflict', *Journal of Strategic Studies*, 46:3 (2023), pp. 570–94.

[8] Ugochukwu Etudo, Christopher Whyte, Victoria Yoon, and Niam Yaraghi, 'From Russia with fear: Fear appeals and the patterns of cyber-enabled influence operations', *Journal of Cybersecurity*, 9:1 (2023), tyad016.

[9] Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec (eds), *Information Warfare in the Age of Cyber Conflict* (London: Routledge, 2021).

[10] Etudo et al., 'From Russia with fear'.

[11] Among others, Diego A. Martin, Jacob N. Shapiro, and Julia G. Ilhardt. 'Introducing the online political influence efforts dataset', *Journal of Peace Research*, 60:5 (2023), pp. 868–76; Brandon Valeriano and Benjamin Jensen, 'Innovation and the

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

Unpacking cyber-enabled influence

How do cyber attacks aid attempts to generate influence? On the face of it, we might expect many experts to argue that they really don't. After all, as will be explained below, the logic of both activities for political purposes as laid out in various kinds of scholarly analyses is generally quite distinct. Cyber operations, while occasionally used to degrade national security capabilities, typically follow the format of intelligence operations in that they emphasise access, compromise of systems, and secrecy to achieve strategically valuable goals (e.g. intellectual property (IP) theft, systems degradation, or performative sabotage).[12] Influence operations, by contrast, manipulate and corrupt information conditions to achieve persuasive effects (for the purposes of political deception, distraction, or something else).[13]

While there are similarities, the operational shape of cyber and influence operations thus ends up being quite distinctive. Both need secrecy for success, for instance. With IO, however, secrecy is not a strict requirement so much as a condition needed in some quantity relative to others. It generally matters much more after an attack is launched due to the need to create sustained effects, with the opposite often being more typically true for cyber activities. Likewise, while cyber operations subvert systems by making them act in ways not intended by defenders, the mechanisms of doing so are syntactic or rely on narrow social engineering attacks. Access, in other words, is possible via manipulation of tangible systems. IO also seek to subvert, but 'compromise' and 'access' are psychological outcomes, at least above the level of campaign tactics. You can hack a social media account, but actual influence requires shaping the information environment via less direct methods of socio-political messaging. And this is something made all the harder by the aforementioned need by the attacker to avoid revealing their involvement. After all, unmasking fundamentally risks the credibility of an IO's messaging, something that is not always true for cyber activities. The result is a discrete pair of mechanisms for conducting interference whose intersection remains critically underspecified.

The intersection of cyber and influence

Before moving forward, it is necessary that we briefly elaborate on the conflation of terminology that characterises work in this space so as to position our work between existing approaches. Specifically, at present, discourse is filled with somewhat confusing terminology like 'cyber influence operations'[14] or 'election hacking'[15] that often conflates two separate kinds of interference and

proper context of cyber operations', *Marine Corps Gazette* (2021), 39–43; and Colin Foote, Ryan C. Maness, Benjamin Jensen, and Brandon Valeriano, 'Cyber conflict at the intersection of information operations: Cyber-enabled information operations, 2000–2016', in Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec (eds), *Information Warfare in the Age of Cyber Conflict* (Routledge, 2020), pp. 54–69.

[12] Max Smeets, 'The strategic promise of offensive cyber operations', *Strategic Studies Quarterly*, 12:3 (2018), pp. 90–113. Also see Florian J. Egloff and James Shires, 'Offensive cyber capabilities and state violence: Three logics of integration', *Journal of Global Security Studies*, 7:1 (2022), ogab028; and Erica D. Borghard and Shawn W. Lonergan, 'Cyber operations as imperfect tools of escalation', *Strategic Studies Quarterly*, 13:3 (2019), pp. 122–45.

[13] Herbert Lin and Amy Zegart (eds), *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Brookings Institution Press, 2019); Herbert Lin, 'The existential threat from cyber-enabled information warfare', *Bulletin of the Atomic Scientists*, 75:4 (2019), pp. 187–96.

[14] Sean Cordey, 'Cyber influence operations: An overview and comparative analysis', CSS Cyberdefense Reports (2019); Jerry M. Couretas, 'Cyber influence operations', in *An Introduction to Cyber Analysis and Targeting* (Cham: Springer, 2022), pp. 57–89; and Trishana Ramluckan, Alicia Wanless, and Brett van Niekerk. 'Cyber-influence operations: A legal perspective', in *Proceedings of the 18th European Conference on Cyber Warfare and Security* (2019), pp. 379–88

[15] Christopher Whyte, 'Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare', *Journal of Cybersecurity*, 6:1 (2020), tyaa013; Jonathan K. Sawmiller, 'Fighting election hackers and trolls on their own turf: Defending forward in cyberspace', *Idaho Law Review*, 56 (2020), pp. 281–294; and Isabella Hansen and Darren J. Lim, 'Doxing democracy: Influencing elections via cyber voter interference', *Contemporary Politics*, 25:2 (2019), pp. 150–71.

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

compromise.[16] As a result, we often don't get a clear view of what that might mean because of overfocus by scholars and practitioners on acts that are actually more one thing than the other.

This tendency represents the primary body of work on what includes, but is not limited to, research on cyber-enabled influence activities. As others have noted,[17] work in this area relies on a range of terms rooted in diverse operational, historical, cultural-institutional, and strategic contexts in order to generally describe the 'use of various elements of a state's arsenal of foreign interference and influence in service of strategic objectives, including the employment of limited military force, utilization of intelligence assets, and disruption of both social and political processes via propaganda'.[18] Relevant terms in this space are diverse and often used interchangeably. Following Russian efforts to interfere in the American presidential election season of 2016[19] – undoubtedly the defining moment in the past decade's refocus on malign influence activities by social science researchers – terms like 'election hacking'[20] and 'foreign meddling'[21] have become popular touchpoints for public intellectuals who seek to introduce general publics to the concept of political warfare or even the 'active measures',[22] 'hybrid warfare',[23] or 'psychological warfare'[24] that are the preferred frames deployed by key Western adversaries. In doing so, conversation about foreign malign influence has more easily connected with broader discourse on propaganda and disinformation in the age of the internet.

We see this tendency even in recent scholarship that looks to cyber conflict as sensitive to the transformative effects of digital infrastructures on the potential of influence activities. Vicic and Gartzke argue that influence effects are often more decisive for political outcomes than the flashy destructive hacks often hyped in popular imagination, highlighting that many operations blur technical and psychological modalities in pursuit of political outcomes.[25] Likewise, Gomez emphasises how the digital environment amplifies the scale and targeting precision of traditional influence strategies, framing the 'medium effects' of cyberspace as transformative.[26] And Shires, analysing

[16] There is also a broad body of work in the communications, psychology, Science, Technology & Society (STS), and information systems areas that variably utilises this terminology in studies that examine social media manipulation, coordinated trolling, etc. See, for instance, Savvas Zannettou, Tristan Caulfield, Emiliano De Cristofaro, Michael Sirivianos, Gianluca Stringhini, Jeremy Blackburn, Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web, WWW '19: Companion Proceedings of The 2019 World Wide Web Conference, pp. 218–226; Savvas Zannettou, Michael Sirivianos, Jeremy Blackburn, and Nicolas Kourtellis, 'The web of false information: Rumors, fake news, hoaxes, clickbait, and various other shenanigans', *J Data Inf Qual*, 3:11 (2019), pp. 1–37; A. Kim and A. R. Dennis, 'Says who? The effects of presentation format and source rating on fake news in social media', *MIS Q Manag Inf Syst*, 43 (2019), pp. 1025–39; and W. L. Bennett and S. Livingston, 'The disinformation order: Disruptive communication and the decline of democratic institutions', *Eur J Commun*, 33 (2018), pp. 122–39.

[17] Etudo et al., 'From Russia with fear'; Jelena Vićić and Richard Harknett, Identification-imitation-amplification: understanding divisive influence campaigns through cyberspace. *Intell National Security*, 39:5 (2024), pp. 897–914.

[18] Whyte et al. (eds), *Information Warfare in the Age of Cyber Conflict*.

[19] Kathleen Hall Jamieson, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know* (Oxford University Press, 2020); Kathleen Hall Jamieson, 'How Russian hackers and trolls exploited US media in 2016', *Proceedings of the American Philosophical Society*, 163:2 (2019), pp. 122–35; and Malcolm Nance, *The Plot to Hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election* (Simon & Schuster, 2016).

[20] Alexander Leveringhaus, 'Beyond military humanitarian intervention: From assassination to election hacking?', *Philosophical Journal of Conflict and Violence*, 5:1 (2021), pp. 109–28.

[21] David V. Gioe, 'Cyber operations and useful fools: The approach of Russian hybrid intelligence', *Intelligence and National Security*, 33:7 (2018), pp. 954–73.

[22] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Farrar, Straus and Giroux, 2020).

[23] William Steingartner and Darko Galinec, 'Cyber threats and cyber deception in hybrid warfare,' *Acta Polytechnica Hungarica*, 18:3 (2021), pp. 25–45; C. S. Chivvis, 'Understanding Russian "hybrid warfare"', Rand Corporation (2017), p. 17; and Sorin Dumitru Ducaru, 'The cyber dimension of modern hybrid warfare and its relevance for NATO', *Europolity-Continuity and Change in European Governance*, 10:1 (2016), pp. 7–23.

[24] Benjamin Jensen, 'The cyber character of political warfare', *The Brown Journal of World Affairs*, 24:1 (2017), pp. 159–72.

[25] Vicic and Gartzke (2024).

[26] Miguel Alberto Gomez, 'Cyber-enabled information warfare and influence operations: A revolution in technique?', in Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec (eds), *Information Warfare in the Age of Cyber Conflict* (Routledge, 2020), pp. 132–146.

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

hack-and-leak campaigns, shows how tactical intrusions and strategic influence are tightly fused in contemporary practice.[27] These contributions move the field forward by clarifying how influence operations can be cyber-enabled. However, they also reflect the broader trend of reinterpreting cyber incidents through an influence lens, sometimes without consistently delineating how cyber means relate to influence ends and regularly incorporating the shift towards influence outcomes as part and parcel of cyber conflict as a distinct conceptual arena of activity and study.

Prominent policy and research organisations have echoed this tendency. Cordey, for instance, defines cyber influence operations as illegitimate uses of cyber capabilities to shape perceptions, choices, or emotions. This explicitly unites technical exploits and informational manipulation under a single cyberspace-centric conceptual heading.[28] Mazarr et al.'s work on hostile social manipulation similarly frames cyber capabilities as instruments of coordinated disinformation and perception management.[29] These definitions signal growing recognition of the integrated character of CEIO. Yet even as these perspectives help formalise a hybrid category, they risk further entrenching ambiguous usage by describing a wide range of actions – spanning system intrusion, data theft, narrative amplification, and social engineering – as part of the same continuum, often without disambiguating their distinct dynamics.

This article builds on that evolving conversation while making a more explicit effort to clarify terms and specify mechanisms. Where existing treatments sometimes assume the unity of cyber and influence elements, the typology introduced here seeks to isolate different modes of coordination and targeting across the CEIO spectrum. The aim is not to artificially separate domains that are increasingly intertwined, but rather to bring sharper analytical resolution to how cyber means are used to achieve influence effects. In doing so, this article addresses ongoing ambiguity in the literature and contributes to a more structured account of cyber-enabled influence operations as a distinct – though variegated – category of strategic behaviour. Of particular note, within this broad realignment of focus on influence as a tool of statecraft, the cyber operational augmentation of influence activities has often been derailed by an aberrant acknowledgement that IO are increasingly made most effective by actions taken in or via cyberspace.[30] The result has generally been treatment of 'cyber influence operations' that make (relatively) light of the connection between what are otherwise treated by scholars as distinct mechanisms of statecraft. Influence operations certainly find amplification in actions enabled by the internet or in societal conditions moulded by the internet.[31] But the actual role of cyber effect activities, such as the deployment of malware or disruptive attacks on infrastructure, for enhancing the strategic utility of digital age IO remains underspecified.[32]

Targeting: Cyber as an adjunct of influence

Juxtaposed to the conflation of cyber and influence activities in much scholarship since the late 1990s is a more recent empirical focus on the targeting of IO, an analytic set of problematics that

[27] James Shires, 'Hack-and-leak operations: Intrusion and influence in the Gulf', *Journal of Cyber Policy*, 4:2 (2019), pp. 235–56.

[28] Cordey, 'Cyber influence operations'.

[29] Michael J. Mazarr, Ryan Michael Bauer, Abigail Casey, S. Heintz, and Luke J. Matthews, 'The emerging risk of virtual societal warfare', in *Social Manipulation in a Changing Information Environment* (Santa Monica CA: RAND Corporation, 2019), p. 353.

[30] E.g. David Tayouri, 'The secret war of cyber influence operations and how to identify them', Institute for National Security Studies Cyber, Intelligence, and Security Publication 4 (2020), pp. 5–22; or Marie Baezner and Sean Cordey. 'Influence operations and other conflict trends', in Dunn Cavelty, Myriam, and Andreas Wenger. *Cyber security politics: Socio-technological transformations and political fragmentatio*. (Taylor & Francis, 2022), pp. 17–31.

[31] Tayouri, 'The secret war of cyber influence operations and how to identify them'; Peter Schrijver and Paul Ducheine, 'Cyber-enabled influence operations', *Militaire Spectator*, (June 14, 2023), 284–295; and Barrie Sander, 'Democracy under the influence: Paradigms of state responsibility for cyber influence operations on elections', *Chinese Journal of International Law*, 18:1 (2019), pp. 1–56.

[32] Etudo et al., 'From Russia with fear'.

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

often involve focus on cyber operations tied to influence efforts. In this limited-but-expanding research programme, CEIO has been given new significance by the broader attempt to understand the structure of internet-enabled IO. Simply put, what dictates the systems, persons, and processes that are targeted by belligerents seeking to deploy influence towards some strategic gain? What shapes the selection of specific services, accounts, and modes of user engagement? And what factors delineate the themes, issues, and approach to messaging that will operationally elevate such tactical activity to produce strategically favourable outcomes?

Work in this area that is relevant to CEIO takes two primary forms. The first is data collection efforts to align understanding of cyber and influence activities. Work on Valeriano et al.'s Dyadic Cyber Incidents and Disputes dataset,[33] for instance, has noted the conduct of information warfare practices occurring contemporaneously with cyber operations since 2020. Martin et al.'s political influence dataset likewise ties the two together by recording the involvement of foreign advanced persistent threat actors (APT) in influence campaigns.[34] While it's notable that these efforts do not speak directly to the utility of cyber operations for influence operation activities, they nevertheless illustrate a clear overlap in the methods being deployed for broadly similar purposes by interfering foreign belligerents.

The second area of work on IO targeting is the recent series of articles that attempt to empirically examine the patterns of engagement by foreign belligerents such as the Russian Federation, Iran, and China.[35] Works like Etudo et al. (2023)[36] and Vicic and Gartzke (2024)[37] attempt to adjudicate between a set of hypotheses about what factors guide the progress of influence activities by such actors. Generally, there is an assumption that IO are tactically more nuanced than a high-level overview of national interests.[38] Given this, are IO simple tools of division designed to exacerbate societal fault lines wherever they can be found for purposes of strategic distraction?[39] Are IO shaped by case-specific intelligence conditions and outcomes? Perhaps the shape of IO witnessed during the 2010s and 2020s so far has more to do with the institutional context of organisations like Russia's GRU[40] than with more generalisable strategic touchpoints. Or do IO have few consistent structures, instead constituting inevitable learning life cycles that produce coherent patterns of approach in their latter stages?

For questions of utility, targeting, and more, these areas of scholarship have yet to reveal much about the actual empirical footprint of CEIO. One exception to this is the discovery by Etudo et al. of malware injected into a secondary phase of influence efforts to capture vulnerable populations for further manipulation during the 2014–16 Internet Research Agency (IRA) campaign against

[33] Foote et al., 'Cyber conflict at the intersection of information operations'; Bryan James Nakayama, 'Information vs the cyberspace domain', *Journal of Cyber Policy*, 7:2 (2022), pp. 213–29.

[34] Martin et al., 'Introducing the online political influence efforts dataset'; also see Diego A. Martin and Jacob N. Shapiro, 'Trends in online foreign influence efforts' (2019); and Diego Martin, Jacob N. Shapiro, and Michelle Nedashkovskaya, 'Recent trends in online foreign influence efforts', *Journal of Information Warfare*, 18:3 (2019), pp. 15–48.

[35] Building on initial work such as Lucan Ahmad Way and Adam E. Casey, 'How can we know if Russia is a threat to Western democracy? Understanding the impact of Russia's second wave of election interference', in *Conference on Global Populisms and Their International Diffusion* (2019).

[36] Etudo et al., 'From Russia with fear'.

[37] Vicic & Gartzke (2024).

[38] A point backed up by Benjamin Jensen, Brandon Valeriano, and Sam Whitt. How cyber operations can reduce escalation pressures: Evidence from an experimental wargame study. *J Peace Res*, 61:1 (2024), pp. 119–133.

[39] Of note, this article does not assume that all IO aim at division as a matter of course but rather vary in scale and scope depending on the character and position of actors involved, whether nation-states (e.g. pariah states like Russia post-2022 or rules-focused revisionist states like China) or different kinds of socio-political actors (e.g. strict ideological political elements vs truly fringe extremists). The scope of our description of IO as augmented by cyber activities is thus agnostic, not directed at one type or another but the full range of actors that simply aim to achieve artificial informational effects regardless of their nature. The primary caveat we make is that our arguments herein surrounding the utility of public-facing cyber and influence actions will inevitably vary depending on the sensitivity of governing structures to popular factors, meaning that this framework is most analytically useful for the case of counter-democracy CEIO.

[40] Fully, the Main Directorate of the General Staff of the Armed Forces of the Russian Federation or Glavnoye Razvedyvatel'noye Upravleniye (GRU).

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

the United States.[41] More systematic analysis of cyber operations in such contexts has yet to be conducted. Nevertheless, these two wings of relevant work do offer a compelling basis for better examination of the confluence of cyber and influence activities. Specifically, there is evidence in each of the studies referenced that the logic of the primary activity – that of attempts to manipulate and corrupt information conditions to achieve persuasive effects – shapes adjunct operational deployments. We start from this assumption and build an analytic framework for seeing the interaction of cyber and influence operations, not as a singular phenomenon grounded in an overriding logic of information warfare but rather as a dynamic interaction of operational toolkits that sees distinct modes of deployment based on evolving target conditions.

Four levels of cyber-enabled influence

Scholars acknowledge that cyber operations are anything but blunt mechanisms for interstate signalling or deterrent posturing.[42] Rather, cyber operations reflect tailorable general purposes capabilities for intelligence gathering, sabotage, subversionl and narrow degradation of national security capacities. In the International Relations (IR) literature on cyber conflict, a debate rages as to the precise logic of cybersecurity for interstate engagement. Is it a glorified intelligence contest[43] or a more direct reflection of state's strategic preferences?[44] Despite this debate, conversation about cyber operations as an adjunct modifier of other methods of interstate engagement sometimes fails to reflect the context of functional nuance. As already alluded to, examinations of 'cyber influence operations' or even some more direct recent studies of CEIO simply see the two forms of engagement as connected by the digital domain, a curiosity in itself given the inherent conceptual artificiality of cyberspace and its relatively exclusive use by Western societies.

While there is nothing wrong with the interchangeable use of 'cyber' terminology to talk about either influence or network activities among pundits, we argue that thinking explicitly about the utility of cyber methods for augmenting influence activities demands a framing of the former around the operational footprint of the latter and greater clarity about the kinds of augmentation involved. As such, we outline four distinct kinds of CEIO that are not defined by technique or national interests or the context of other cyber activities an actor might undertake. Rather, they speak to different levels on which influence might be generated. These are:

- **Preparatory attacks:** activities that leverage the intelligence potential of cyber attacks to enhance the potential of a subsequent influence campaign. Those actions include reconnaissance, resource (e.g. botnets) creation, account takeover, directed capacity denial, and targeted socio-political compromise.
- **Manipulative attacks**: these are intended to create influence in themselves (e.g. by compromising voter systems).
- **Attacks in parallel**: these involve cyber activities leveraged against a nation simultaneously with influence activities without clear operational coordination (e.g. a disruption of government services undertaken during a campaign to influence election primaries via coordinated disinformation).
- **Influence-enabling attacks**: these reverse the conventional logic of CEIO and see interference activities leveraged to augment the socio-political impact of cyber operations (e.g. compromise of state-level voter databases on an election day where public panic results if amplified

[41] Etudo et al., 'From Russia with fear'.

[42] Thomas Rid, 'Cyber war will not take place', *Journal of Strategic Studies*, 35:1 (2012), pp. 5–32; Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford University Press, 2018); and Erik Gartzke, 'The myth of cyberwar: Bringing war in cyberspace back down to earth', *International Security*, 38:2 (2013), pp. 41–73.

[43] Zegart et al., *Deter, Disrupt, Or Deceive*.

[44] Fischerkeller et al., *Cyber Persistence Theory*.

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

by preceding concentric influence campaigns to generate both distrust in government capacity to secure election systems and suspicion of foreign collusion on the part of specific elite or fringe socio-political actors).

In this imagining of the intersection of cyber-enabled influence activities, influence is created via the intercession of cyber means in several distinct ways.

Preparatory attacks

First, preparatory attacks describe a broad range of activities that aim to strengthen the conventional mechanisms of influence activities, including social media manipulation and conventional media interference, targeted political messaging via non-digital avenues of engagement, the priming of elite populations to support some influence campaign objective, and more. While the literature on cyber-enabled influence has thus far set its gaze at a level of analysis above this, there is nevertheless immense evidence of such activities in scholarship, in professional and security reporting, and in punditry.

Notably, in recent scholarship, Etudo et al.'s reveal of malware used in tandem with social media messaging designed to capture vulnerable populations and then expand population parameters via a blended cyber-influence mechanism of click fraud is a significant example.[45] Elsewhere, there is perhaps most clear evidence of extensive intrusion activity linked to influence operations that are about pre-operational reconnaissance and the furnishing of intelligence.[46] This naturally extends to resource creation activities as well, such as the creation of botnets or of Potemkin villages such as networks of compromised websites that can be used to shape influenced communities of users.[47] On another front, Forest and Diehl suggest that tactical cyber intrusion activity is a valuable tool for creating noise that distracts technology providers and watchdogs from other malign use of media platforms as initial beachheads are being developed by foreign belligerents.[48] Likewise, while these initial beachheads supporting IO might involve organic account creation en masse, it may also include unsophisticated cyber actions that strengthen the potential for parasocial network development during an IO,[49] including account takeovers.[50] Finally, cyber intrusion tied to an IO might involve the socio-cognitive targeting of elites or of the capacity of technical services prior to the launch of a population-centric phase of interference, both of which may be designed to improve the chances of unfettered engagement with a foreign population.[51]

Preparatory attacks are often difficult to see absent hindsight given that many intrusion activities could yield a number of potential secondary benefits in the future or none at all. However, recent major cyber incidents at the time of writing include a number of possible candidates for broader CEIO. These include Chinese cyber espionage activities via the threat actor Salt Typhoon against American telecommunications infrastructure through 2024, in which access could certainly underwrite future influence operations.[52] This set of campaigns parallels several targeting

[45] Etudo et al., 'From Russia with fear'.

[46] For work in the area more broadly, see Gaute Wangen, 'The role of malware in reported cyber espionage: A review of the impact and mechanism', *Information*, 6:2 (2015), pp. 183–211.

[47] Patricia Bailey, 'Online Potemkin villages: Discovering a Russian influence operation on social media', *Cyber Security: A Peer-Reviewed Journal*, 7:3 (2024), pp. 262–72.

[48] Forrest Hare and William Diehl, 'Noisy operations on the silent battlefield', *The Cyber Defense Review*, 5:1 (2020), pp. 153–68.

[49] Christopher Whyte, 'Of commissars, cults and conspiratorial communities: The role of countercultural spaces in "democracy hacking" campaigns', *First Monday* (2020).

[50] Wolfgang G. Stock, Katrin Scheibe, and Franziska Zimmer, 'Cyber social interactions: Information behavior in between social and parasocial interactions' (2022). *J Inf Sci Theory Pract,* 10:3 (2022), pp. 15–23.

[51] Christopher Whyte, 'Beyond tit-for-tat in cyberspace: Political warfare and lateral sources of escalation online', *European Journal of International Security*, 5:2 (2020), pp. 195–214.

[52] 'Chinese Salt Typhoon cyberespionage targets ATT networks, secure carrier says', Reuters (29 December 2024), https://www.reuters.com/technology/cybersecurity/chinese-salt-typhoon-cyberespionage-targets-att-networks-secure-carrier-says-

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

South-east Asian nations in the same period. Iran, Russia, and North Korea similarly undertook preparatory campaigns between 2023 and 2024. Tehran's hackers conducted intrusions and created assets that were then used to amplify pro-Hamas rhetoric, much of which occurred in the information spaces of Gulf nations,[53] and hackers tied to the Kremlin attacked various NGOs linked to anti-Russia issue positions to steal sensitive data.[54] North Korean hackers, for their part, were implicated in a series of low-level compromises of South Korean media infrastructure without (at the time of writing) follow-on disruption.[55]

Manipulative attacks

Cordey (2019) demonstrates that narratives are central to the strategic utility of CEIO, as they link the psychological effects of influence operations with the technical affordances of cyber intrusions. This supports the categorisation of 'preparatory attacks' as foundational to CEIO success.[56] The second category of influence generated via the intercession of cyber means, however, is the one most often referenced by scholars in both regular discourse about CEIO and in recorded data resources on cyber conflict – *manipulative* attacks.[57] They are also perhaps the simplest to understand in terms of their potential utility. Manipulative attacks involve direct attempts to generate the conditions of malign influence on behalf of a belligerent actor. This may include, among other things, attempts to gain access to voting records databases or other election infrastructure, to directly poison or otherwise impact information search algorithms deployed by social media platforms,[58] or to performatively disrupt a socio-political actor (meaning the second-order creation of utility from the theatre surrounding an operation in addition to the functional effects).[59] In each instance, a cyber intrusion event directly impacts the perspective of information consumers in a target nation. Targeting election infrastructure, for instance, might be a preparatory attack if an intrusion can maintain secrecy and provide population-based intelligence. But a more visible attempt at such compromise may create distrust in the integrity of voting systems or otherwise impact prevailing domestic narratives about election processes.[60]

The same is true for attempts to compromise the algorithmic infrastructure that is so important to the conduct of democratic discourse in the 21st century or for visible interference with domestic socio-political operatives. After all, as authors like Bennett and Livingston and Whyte argue,[61] the

2024-12-29/; and "State–Backed China Hackers Targeting South China Sea Claimants, US Cyber Firm Says." Radio Free Asia, (9 Dec. 2021), Radio Free Asia, https://www.rfa.org/english/news/china/hackers-southchinasea-12092021103242.html

[53] 'Iran surges cyber-enabled influence operations in support of Hamas', Microsoft Security Insider Intelligence Reports (2023), https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas/; and 'Iranian cyber activities in the Gulf states: Espionage on the rise', BBC News (2022), https://www.bbc.com/news/world-middle-east-cyberespionage.

[54] 'Information warfare: China, Russia, and influence operations involving NGOs', Riley Sentinel (2024), https://rileysentinel.com/information-warfare-china-russia-and-influence-operations-involving-ngos/.

[55] 'North Korea hacks South Korean media networks', *Korea Herald* (2023), https://www.koreaherald.com/north-korea-cyberattacks-south.

[56] Cordey, 'Cyber influence operations'.

[57] E.g. James Scott, Drew Spaniel, and Rob Roy, *Hacking Elections is Easy!*, Institute for Critical Infrastructure Technology (2016); Thomas Rid and Ben Buchanan, 'Hacking democracy', *SAIS Rev of Int Aff*, 38 (2018), pp. 3–16; and Scott J. Shackelford, Bruce Schneier, Michael Sulmeyer, et al., 'Making democracy harder to hack', *University of Michigan Journal of Law Reform*, 50 (2016), pp. 629–668.

[58] Christopher Whyte, 'Poison, persistence, and cascade effects', *Strategic Studies Quarterly*, 14:4 (2020), pp. 18–46.

[59] We use the term 'performative' in this article to denote the strategic and operational utility to be accrued from the second order theatre of influence or cyber activities, similar in shape to those sought by terrorist actors in their attempt to generate coercive effects via publicity surrounding attacks. See Gabriel Weimann, 'The theater of terror: The psychology of terrorism and the mass media', *Journal of Aggression, Maltreatment & Trauma*, 9:3–4 (2005), pp. 379–90.

[60] Michael Chertoff and Anders Fogh Rasmussen, 'The unhackable election: What it takes to defend democracy', *Foreign Affairs*, 98 (2019), pp. 156–164.

[61] W. Lance Bennett and Steven Livingston, 'The disinformation order: Disruptive communication and the decline of democratic institutions', *European Journal of Communication*, 33:2 (2018), pp. 122–39; Christopher Whyte, *Subversion 2.0: Leaderlessness, the Internet, and the Fringes of Global Society* (Oxford University Press, 2024).

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

architecture of social media platforms amplifies disinformation through algorithmic promotion of sensationalist content. This reinforces the utility of manipulative attacks in helping to target vulnerable audiences, such as through algorithmic poisoning or false narrative amplification. Moreover, as Kim and Dennis highlight, the framing of information, combined with perceived credibility, can significantly affect its uptake.[62] This underscores why manipulative attacks that target search infrastructure underlying algorithms and social media environments require a sophisticated understanding of user behaviour and content dissemination strategies.

The empirical record is replete with instances of such manipulative attacks, most recently broad-scoped efforts to interfere with elections in 2024 in both Western and non-Western settings. Extensive reporting exists on the actions of Russia, China, and Iran taking direct cyber-operational steps to generate influence effects in Europe and North America during the period.[63] Elsewhere, state-sponsored cyber actors launched attacks on election infrastructure in Myanmar to alter voter data, aiming to influence election outcomes in favour of military-backed candidates, and also conducted manipulative attacks on social media platforms in the Philippines and against voting systems in Nigeria, spreading disinformation and creating disruptions to influence public perception during election life cycles.[64]

Attacks in parallel

Third, though relatedly, CEIO may be constituted of attacks undertaken *in parallel* to IO activities. Consider a scenario in which two closely aligned democratic nations share an election year and in which races for national leadership in both feature candidates that are outspoken about a foreign conflict, such as Russia's war against Ukraine or Iranian support of Houthi rebels in the Persian Gulf.[65] In this case, sudden attacks designed to disrupt the campaign activities of one such candidate on the eve of an election may produce influence outcomes in the second state, perhaps convincing political planners to moderate their messaging. Other scenarios where parallel activities create signalling effects for either elites or publics (foreign or domestic) are equally imaginable, for instance, creating noise to distract domestic populations or change their view of an organisation's credibility.

In this category, the empirical record suggests a coordination without operational tie-in across Russian disinformation campaigns in Europe between 2022 and 2024 for attacks such as the downing of Italian government websites and Ukrainian critical infrastructure in 2024.[66] The actions of Indian and Pakistani threat actors surrounding periods of cross-border tension in which cyber groups from both nations conducted attacks on each other's government websites while parallel influence campaigns promoted nationalistic narratives domestically also fit the remit,[67] as

[62] Antino Kim and Alan R. Dennis, 'Says who? The effects of presentation format and source rating on fake news in social media', *Management Information Systems Quarterly*, 43:3 (2019), pp. 1025–39.

[63] See 'Iranian hackers ramp up influence operations ahead of 2024 U.S. eection', CSO Online (2024), https://www.csoonline.com/article/3586041/iranian-hackers-ramp-up-influence-operations-ahead-of-2024-us-election.html; Wikipedia Contributors, 'Chinese Interference in the 2024 United States Elections.' Wikipedia (December 2024), https://en.wikipedia.org/wiki/Chinese_interference_in_the_2024_United_States_elections.

[64] See "Myanmar's Digital Coup Rigging the Election before It Begins", 18 Mar. 2025, humanrightsmyanmar.org/elections-during-myanmars-digital-coup/; Quitzon, Japhet. "Social Media Misinformation and the 2022 Philippine Elections," Center for Strategic and International Studies, (22 November 2021), www.csis.org/blogs/new-perspectives-asia/social-media-misinformation-and-2022-philippine-elections; Izuaka, M, 'Nigeria recorded 12.9 million Cyberattacks during presidential, NASS elections – Minister', Premium Times, (23 March 2023), https://www.premiumtimesng.com/business/business-news/587712-nigeria-recorded-12-9-million-cyberattacks-during-presidential-nass-elections-minister.html.

[65] Not indistinct from that described in Erica D. Lonergan and Shawn W. Lonergan, 'Cyber operations, accommodative signaling, and the de-escalation of international crises', *Security Studies*, 31:1 (2022), pp. 32–64.

[66] Center for Strategic and International Studies, 'Cyber operations during the Russo-Ukrainian war', CSIS Analysis (2024), https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

[67] 'India–Pakistan cyber tensions escalate amid cross-border disputes', *Hindustan Times* (2021), https://www.hindustantimes.com/india-pakistan-cyber-tensions.

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

do cyber-enabled disruptions in Hong Kong in 2019 in parallel with disinformation targeting pro-democracy organisations[68] and attacks conducted against Ethiopian government communication systems in 2021 at the same time influence campaigns sought to manipulate international sentiment around the Tigray conflict.[69]

Influence-enabling attacks

Finally, cyber operations may be used as the primary mechanism of spreading influence pursuant to an influence campaign designed to securitise cybersecurity vulnerability (i.e. an *influence-enabling* attack). Unlike a manipulative attack where the target of a cyber activity dictates the inherent influence value of the activity (and is thus a highly functional undertaking), in this category of CEIO the cyber operation may take any form. This is because influence is generated not by the activity itself, but by the conditions of expectation set by a foregoing IO. While this category of CEIO is arguably the rarest, there is evidence to suggest that influence is generated along these lines. For example, statements made by the leaders of Russia and Iran about the need to deploy asymmetric activities against Western society targets appear to result in greater sensitivity to disruption of critical infrastructure targets among those populations. In this way, influence primes cyber operations to take on an additional dimensionality in creating informational effects beyond what most CEIO involves, such as in the case of Iran's selective take-down of anti-Hamas accounts following propaganda activities in 2023 or similar disruption of activist organisations by Egypt and Turkey after tailored disinformation campaigns were undertaken (i.e. a 'smear, then snare' tandem operation to discredit, then eliminate).[70]

Building towards CEIO theory

In this section, we link the categorisation of CEIO outlined above to the logical foundation of digital-age foreign malign-influence campaigns and suggest a theoretical foundation for future analyses of CEIO. Then, in the next section, we preliminarily validate our supposition with a broader survey of the landscape of CEIO in world affairs to complement the case examples offered so far.

Operational interactions: IO vs. cyber

As mentioned previously, recent work on cyber operations in world politics has involved extensive debate as to the utility of digital instruments for signalling and conventional strategic manoeuvring versus more limited adjunct security outcomes, namely intelligence gathering and related compromise activities. Regardless of which perspective a given scholar supports, there is a robust consensus among academics stretching all the way back to Rid's seminal work on the subject that cyber activities present an operational logic centred on subversive gains realised via the manipulation of informational circumstances, both semantic and syntactic.[71]

In terms of the logic of cyber operations, Maschmeyer describes the promise of cyber operations as about overcoming four distinct operational challenges.[72] These comprise (1) identifying suitable vulnerabilities for exploitation in systems that are designed by others (and indeed may

[68] 'Cyberattacks target pro-democracy groups amid Hong Kong protests'. *South China Morning Post* (2019), https://www.scmp.com/news/hong-kong-protests-cyberattacks.

[69] 'Cyber attacks during Ethiopia's Tigray conflict complicate peace efforts', *The Guardian* (2021), https://www.theguardian.com/world/ethiopia-cyber-attacks-tigray.

[70] 'Iran surges cyber-enabled influence operations in support of Hamas'; 'Turkey's cyber efforts against Kurdish groups intensify', Anadolu Agency (2021), https://www.anadoluagency.com/turkey-cyber-operations-kurds; and 'Egyptian cyber attacks on journalists spark international outcry', Reuters (2022), https://www.reuters.com/article/egypt-journalist-cyber-surveillance.

[71] Rid, Thomas. "Cyber war will not take place." *Journal of strategic studies* 35.1 (2012), pp. 5–32.

[72] Lennart Maschmeyer, 'The subversive trilemma: Why cyber operations fall short of expectations', *International Security*, 46:2 (2021), pp. 51–90.

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

be further modified and customised by intermediary users), (2) exploiting said systems without being detected, (3) establishing access and control over systems without being detected, and (4) maintaining systems control sufficient to produce effects that correspond to attacker outcomes. It is generally these potential outcomes that are the subject of debate on the strategic utility of cyber operations, with advocates on either side variably seeing limitations (or not) on manipulation of network infrastructure and the processes tied thereto leading to strategically useful effects. Regardless, these functional challenges remain the same across the board. Maschmeyer further suggests that the main defining feature of operational deployment comes in the form of a trilemma, where operational effectiveness is perennially constrained in terms of the speed, intensity, and control possible with cyber activities.[73] Simply, these attributes of cyber operations are negatively correlated, with rapid action correlated with less potent outcomes and shakier control conditions, high-intensity effects requiring slower build-up, and so on.

One might argue that IO achieve their promise by overcoming the same challenges. After all, as others have argued, national societies – inclusive of systems of governance, communal social and economic engagement, commerce, and more – are a form of complex information system. That being said, it is critical that we recognise that the characteristics of that system and of the nature of social subversion are distinct enough from that of network infrastructure to alter the operational realities of IO. As such, it is worth considering the operational logic of IO as one that abuts that of cyber operations but references alternative real-world conditions that influence the planning, implementation, and eventual utility thereof.

First, it is absolutely true that IO (both under the specific definition offered herein and under alternative designations) must identify suitable vulnerabilities in a target system for exploitation as a precursor to the generation of influence. However, the system in question defines both the nature of the vulnerability and the meaning of 'suitable' opportunities for exploitation. With IO, the focus of exploitation is inevitably broader than most cyber operations insofar as the systems to be subverted are socio-political and economic in nature. These societal processes are underwritten by the same network architecture that is targeted by any cyber activity, but only in part. They are also constituted in semantic informational complexities that are shaped by factors beyond the management of information systems and are resultantly prone to rapid and often more unexpected transformations (by, for instance, emergent socio-political narratives or commercial market developments).[74] The result is fault lines that might be expanded or mitigated by change that is exogenous to the point of contact between IO and target societies.[75]

Second, IO must also exploit discovered vulnerabilities without detection. As with cyber operations, secrecy is a critical element of generating access to a target information system (regardless of the differences in how those information systems are constituted), sustaining that access out towards some intended effect. However, the timing is much different for IO, with secrecy becoming *more* pressing over time as influence is induced and leveraged.[76] Indeed, non-detection is arguably not necessary in a tactical sense prior to the formation of an *operation*, as lack of knowledge of an organised interference effort on the part of the target results in intrusion events appearing as scattered data points. It may even be useful as an exercise in noise generation. Only later, when an organised campaign exists to support attribution analytics, does detection threaten compromise.[77]

Third, while IO must invariably include access to relevant workings of the targeted societal systems involved without detection, the idea of control is much more illusory than with cyber operations. Access for IO is much less clearly about maintaining a capacity to trespass in a space with specific syntactic architecture and more about coordinative potential. IO operators seek to

[73] Lennart Maschmeyer, *Subversion: From Covert Operations to Cyber Conflict* (Oxford University Press, 2024).

[74] Joe Devanny, Ciaran Martin, and Tim Stevens, 'On the strategic consequences of digital espionage', *Journal of Cyber Policy*, 6:3 (2021), pp. 429–50.

[75] Etudo et al., 'From Russia with fear'.

[76] Ibid.

[77] Ibid.

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

generate the potential for injecting information that is foreign to the target system (malign content, sources of narrative generation, etc.) and scale it to produce influence effects and, thereafter, favourable aftershocks (e.g. disinformation that produces additional misinformation). But the outsider-looking-in dynamic of foreign-based IO and the semantic complexities of societal information systems referenced above combine to create a dependency on domestic trigger conditions.[78] The result is that 'control' is a temporally limited condition, an ability to coordinate the generation and proliferation of influence that must be acquired *and reacquired* based on the shifting semantic architecture of the target. As such, a better term than control for what IO belligerents seek might be *centrality* (in the eigenvector sense) defined as the condition of maximal possible connectivity.

Finally, the maintenance of this condition of control/centrality within the target system is certainly desirable for the production of effects that align with belligerent interests. Here too, however, a key difference separates IO and cyber operations. Specifically, unlike cyber operations, IO commonly emphasise what was previously described as *aftershocks*, meaning organic follow-on effects that permit minimal re-engagement relative to maximal strategic gain.[79] This tendency is clear not only in the campaign-level behaviour of malicious influence operators but also in their tactical practices. For instance, as early as influence activities associated with the Brazilian World Cup in 2014, it has been common practice for malicious social media accounts to spread sensationalist information and then remove evidence of their messaging once a pursuant conversation has picked up enough steam of its own.[80] Operationally, this is a desirable outcome that maximises late-stage secrecy during an influence campaign and cedes numerous other organisational benefits, including resource efficiency from a less pronounced active management requirement.

A hybrid logic of CEIO

Taken together, these divergent challenges for the exploitation of societal information systems on the part of IO operators sketch a logic of engagement that, while obviously similar in a broad sense to cyber activities as informational attempts at subversion, is quite distinct. To return to the overarching focus of this article, the question thus becomes: how might we expect to see the logic of cyber operations converge with that of IO sufficiently to allow prediction of the deployment of different cyber techniques in support of influence?

In the theoretical parlance of Maschmeyer's subversive trilemma for cyber activities, an alternative operational dynamic of engagement emerges. First, early stages of IO constitute conditions in which speed of engagement is entirely possible. Intense effects are neither expected nor desired. Centrality is also not required during the early phases of counter-society IO given the general infeasibility of being able to leverage a sufficiently robust foundation of influence to create expansive interference effects. Operational outputs, thus, should be expected to resemble low-intensity activity wherein utility for long-term compromise can be prepared. In other words, *preparatory* cyber activities logically correspond with this phase of IO engagement in a way that others do not. Second, late-phase IO correspond to conditions wherein intensity of effects is desired but control is expected to be limited as described above (particularly after the successful generation of aftershocks). Here, speed of engagement is moot for direct augmentation of the mechanisms of influence generation given the need to avoid unnecessary attribution. But limited engagement surrounding such mechanisms carries fewer risks, motivating speedy *engagement in parallel* provided there is a sufficient return on performative attacks (i.e. one produced by the theatre of the action rather than its direct functional effects). Finally, the conditions of IO suggest that late-phase activities involving extensive operational maintenance of system control/centrality to generate moderate/intense effects only make sense when generated influence is situationally sensitive to

[78] Ibid.

[79] Philip N. Howard, *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives* (Yale University Press, 2020); Philip Howard, Fen Lin, and Viktor Tuzov, 'Computational propaganda: Concepts, methods, and challenges', *Communication and the Public*, 8:2 (2023), pp. 47–53.

[80] Justin P. McBrayer, *Beyond Fake News: Finding the Truth in a World of Misinformation* (Routledge, 2020).

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

informationally sensitive contingencies in the target state. For instance, an influence campaign producing moderate voter suppression effects in a few constituencies becomes a good candidate for direct additional *manipulative attack* even given the enhanced risk of discovery and attribution.

To simplify, the contrasting logics of IO and cyber operations suggest an inverse logic of CEIO targeting between the conventional view of cyber attacks as tools of scalable strategic utility and the intelligence logic thereof. The latter form of cyber engagement aligns most clearly with the conditions and requirements of early-stage IO; by contrast, cyber operations that are performative or intended to create direct informational effects (as opposed to creating the mechanisms for influence generation) align with the changing conditions of late-stage IO, though notably under relatively narrow conditions.

Interacting logics: The significance of clearer thinking on CEIO

There is clear value in scholars and practitioners thinking more clearly about CEIO. These blended operations present in a variety of formats and are subsequently linked to influence effects in a series of different ways. This has been outlined in conceptual and theoretical fashion up to this point, but this final section adds empirical validation of this foundational assertion. While not intended as an exhaustive analysis of the universe of cases of CEIO, a survey of a number of known instances of combined cyber engagement alongside IO backs up the idea that CEIO not only take diverse form but also appear pattern-based. And indeed, an initial review of prominent known cases of CEIO validates the theoretical starting point suggested above, which inversely links the logics of cyber and influence operations, as worthy of further scholarly investigation.

The landscape of CEIO

The landscape of CEIO, for reasons noted in the foregoing sections, is difficult to ascertain in no small part because scholars and professional organisations alike often focus on reporting IO and cyber incidents as distinct events linked to one another less by some analysis of their additive effects than by their similar emphasis on informational compromise. For instance, scholarly reporting by Martin et al. highlights at least 53 nations being targeted in 106 distinct campaigns by coordinated non-domestic IO since 2011.[81] These attacks have been attributed to 31 different nations, though the vast majority of such campaigns are the work of a handful of belligerents. Unsurprisingly the vast majority of targeted nations score high on the Polity IV scale (i.e. democracies) in contrast with their attackers (i.e. anocratic and authoritarian regimes). The involvement of cyber operations, however, is somewhat more difficult to observe, with clear ties to APT known to have previously launched cyber operations in about a quarter of all cases and IO activities launched contemporaneous to other cyber operations in 26.67 per cent of cases.[82]

Anecdotally, there is a wide range of known cases that are the subject of scholarly and professional treatments. Russia's interference in the 2016 American presidential election season, now the subject of a host of scholarly articles, is the paradigm example of IO that involved cyber elements, from low-intensity deployment of malware against thousands of everyday citizens to direct attacks on prominent political party infrastructure.[83] But other notable cases have received attention. Recent work has, for instance, highlighted the activities of non-state actors like the Belarusian

[81] Martin et al., 'Introducing the online political influence efforts dataset'.

[82] Ryan C. Maness, Brandon Valeriano, Kathryn Hedgecock, Jose M. Macias, and Benjamin Jensen, 'Expanding the Dyadic Cyber Incident and Campaign Dataset (DCID)', *The Cyber Defense Review*, 8:2 (2023), pp. 65–90.

[83] 'Report of the Select Committee on Intelligence US Senate on Russian Active Measures Campaigns and Interference in the 2016 US Election', Volume 2: Russia's Use of Social Media with Additional Views (2020), pp. 116–290, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures; and producing *inter alia* Adam Badawy, Emilio Ferrara, and Kristina Lerman, 'Analyzing the digital traces of political manipulation: The 2016 Russian interference Twitter campaign', 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), August 2018, pp. 258–65, https://doi.org/10.1109/ASONAM.2018.8508646; Aaron C. Brantly 'A brief history of fake: Surveying Russian disinformation from the Russian Empire through the Cold War

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

Cyber Partisans (BCP) in using cyber attacks to compromise government databases or disrupt infrastructure control systems in order to generate positive coverage of their grievances alongside more common influence activities.[84] More conventionally, Russian engagement of European democracies through the 2010s has involved a varied deployment of cyber instruments alongside social media manipulation and other IO mechanisms.[85] In the United Kingdom, targeted attacks on political infrastructure and government websites occurred in the general elections bracketing the Brexit referendum period but were curiously absent during that debate and the Scottish referendum period that preceded it.[86] In Montenegro, Russian cyber activities have been extensive across at least four different years of political interference, a contrast with the lack of cyber engagement during IO targeting Italian and Bulgarian socio-political processes in the same period.[87] In the Czech Republic, France, Germany, and the Netherlands, cyber attacks have waxed and waned seemingly in line with changing domestic political conditions, either featuring during IO and then dropping away, or vice versa.[88] And beyond Russia, states like Iran and China have increasingly married basic intrusion techniques to create the infrastructure of influence, including extensive social impersonation attacks, use of website injection techniques, etc. to expand networks into which malign content can be poured.

Trends in cyber-enabled influence

The most notable recent research on IO and CEIO more specifically has not only done much to describe the broad shape of influence activities in the 21st century that centre on the internet but has also made much of the temporal character thereof. Etudo et al.,[89] Vicic and Garztke,[90] and others emphasise the cadence and variable momentum of influence engagement over the lifespan of a given campaign. And while there are clearly learning trends to observe in the implementation of CEIO by prominent belligerents in international relations, there are some notable trends in how cyber operations appear – anecdotally – to feature in IO over time.

Perhaps most notable among the various cases noted above is the general draw-down of cyber activities linked to IO that are directly intended to create informational effects via the manipulation of information systems, such as voting infrastructure or social media architecture. While these are common elements of the narrative of Russian interference in the US and the UK between 2014 and 2016, for instance, they do not reappear in the more than two dozen other documented instances of Russian interference campaigns in Europe and North America through the early 2020s aside from two cases (in Netherlands and Germany in 2017). Performative attacks, on the other hand, persist across the period. More tactically, a secondary trend appears to be that new entrants to the CEIO space are utilising intrusion techniques to grow the infrastructure of influence generation in a fashion that quantitatively far exceeds alternative cyber deployments. Iran, for instance, is regularly linked to performative, disruptive cyber operations against targets in the West and across

and to the present', in Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec (eds), *Information Warfare in the Age of Cyber Conflict* (London: Routledge, 2020), pp. 27–41; and German Alvarez, Jaewon Choi, and Sharon Strover, 'Good news, bad news: A sentiment analysis of the 2016 election Russian Facebook ads', *Journal of Communication*, 14 (2020), pp. 3027–53.

[84] Andrei Yu Dudchik, 'Partisans go cyber: The hacker ethic and partisans' legacy' Vestnik of Saint Petersburg University Philosophy and Conflict Studies (2023) 39(2):322-339; and Schrijver and Ducheine. 'Cyber-enabled influence operations'.

[85] Lucan Ahmad Way and Adam Casey, 'Is Russia a threat to Western democracy? Russian intervention in foreign elections, 1991–2017', *Prospects*, 55:6 (2008), pp. 1-13.

[86] Fergus Hanson, Sarah O'Connor, Mali Walker, and Luke Courtois. 'Hacking democracies: Cataloguing cyber-enabled attacks on elections, The Australian Strategic Policy Institute, Policy Brief Report 16 (2019), pp. 1–30.

[87] Anderson, Elizabeth. State–Specific Vulnerabilities to Russian Influence: A Case Study of Montenegro. Master's thesis, Masaryk University, (2019); Darko Trifunović and Darko Obradović, 'Hybrid and cyber warfare-international problems and joint solutions', *National Security and the Future*, 21:1–2 (2020), pp. 23–48.

[88] Ben Buchanan, and Michael Sulmeyer. 'Russia and cyber operations: Challenges and opportunities for the next US administration', Carnegie Endowment for International Peace, 3 (2016).

[89] Etudo et al. (2023).

[90] Vicic and Garztke (2024).

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

the Middle East.[91] However, reporting from Microsoft and other companies that seeks to directly link malicious cyber and influence activity regularly notes operational synergies at the tactical level while distinguishing APT activity against stand-alone targets as one-offs motivated by strategic conditions and current events.[92] This is further contextualised, as a final point, by the fact that relatively greater commitment of interference assets (including dark monies, bot accounts, etc.) appears to be linked to the deployment of cyber techniques against targets of social value rather than those of technical capacity to resist.[93] Taken together, these trends fit the general notion of inverse cyber engagement during IOs theorised based on the framework presented in this article's foregoing sections.

Conclusion: A compelling research programme on CEIO

The need to more thoroughly investigate CEIO is clear. After all, as recent work has emphasised, there is clearly poor systematic understanding of what dictates when and how a state will incorporate cyber capabilities into their influence campaigns. And even more vexingly, no existing work effectively explains why cyber operations linked to IO sometimes don't clearly bolster the informational basis thereof, instead presenting as disruptive interventions that carry risk for the integrity of the influence campaign.

This article has taken first steps to more clearly conceptualise the intersection of cyber and influence operations, activities that share a common information quality but which diverge in their functional logic in key ways. We argue that the key contribution of the framework outlined above, aside from providing greater clarity of examination for scholars in this area, is the initial theoretical supposition it enables that the logic of cyber engagement during IO is likely inversely tied to the functional realities of IO themselves. This point leads on from the assertion found in recent work that the logic of the dominant form of strategic engagement – influence activities targeting societies writ large via primary manipulation of the internet, in this case – shapes the time and manner of the application of supporting methods of statecraft. As a result, this article finds the possibility for greater theoretical clarity about CEIO via a 'third way' between the conflation and granular tactical questioning that, as noted in the introduction, is common in the limited work on the subject in Strategic Studies and related scholarship. As we see it, the analytic separation of cyber and influence effect operations is critical to understanding their confluence and to answering questions about overlapping activity in the grey zone of international relations that are becoming increasingly pressing.

Contributions to theory and practice

This paper establishes a much-needed framework for understanding the intersection of cyber and influence operations, addressing a critical gap in existing scholarship. By differentiating CEIO into four distinct categories – preparatory attacks, manipulative attacks, attacks in parallel, and influence-enabling operations – it provides a structured and replicable model for future research. This framework clarifies often conflated concepts, enabling scholars to better analyse the strategic and operational nuances of CEIO. Furthermore, by demonstrating that 'the style of cyber operational targeting is inversely tied to the scale of influence outcomes', the paper challenges traditional paradigms, offering a novel theoretical lens that integrates cross-domain dependencies and broadens the scope of cybersecurity theory.

The insights presented in this paper also offer actionable guidance for policymakers, strategists, and cybersecurity professionals navigating the complex landscape of CEIO. By distinguishing

[91] Cordey, 'Cyber influence operations'.

[92] Baezner and Cordey, 'Influence operations and other conflict trends'.

[93] Ben Hatch, 'The future of strategic information and cyber-enabled information operations', *Journal of Strategic Security*, 12:4 (2019), pp. 69–89.

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

between the logics underpinning cyber and influence operations, the framework equips decision-makers with tools to assess and counter hybrid threats effectively. The paper's inclusion of diverse case examples, including non-Western and conflict-related CEIO, establishes its applicability for multinational contexts, making it particularly relevant for nations and organisations vulnerable to state and non-state actors. Additionally, the emphasis on domestic conditions shaping CEIO outcomes highlights the critical role of psychological and political resilience in countering digital-age threats.

Overall, we see our work here as about injecting clarity into growing efforts to understand activities at the intersection of cyber and influence operations. By differentiating different forms of interaction between the two types of approach to interference and strategic manoeuvre, we believe that the research programme on CEIO and its core research questions become clearer. A particularly significant element of this contribution is the articulation of cyber operations' utility in the context of information activities, something that should hopefully serve as a basis for broadening discussion of digital threat dynamics beyond the traditional IR-centric field of focus on cyber conflict. We also further discourse on the strategic promise of cyber operations, most distinctly by illustrating how such activities are clearly modified and even redefined in the context of cross-domain operations.

To this point, we provide a basis for alternative thinking about the relationship between tactical campaigning activities and the strategic gain to be generated therefrom that differs from the contemporary signalling-dominant paradigm of persistent engagement in cyber-conflict discourse. Relatedly, we conclude by recognising the particular need to substantially address the primary conceptual drivers of cyber operational practice in the Western defence establishment, notably persistent engagement. Persistent engagement is a strategy that emphasises proactive realisation and mitigation of exploitations.[94] While many have argued that it connotes a shift in posture from the defensive to the offensive, its proponents make great efforts to push back on this worldview for cyber insecurity, arguing instead that offence/defence is a false dichotomy vis-à-vis the need for fluidity of campaign priorities that both cyberspace and the resulting persistence statement imply.[95] Our conceptual work here to develop better thinking on CEIO and the interacting logics of information and cyber operations actually gels well with this mindset. There is certainly an initial critique to be had in the dual-nature identity of CEIO as an instrument of statecraft, namely that cyber outcomes driven by non-cyber logics at the tactical level make the effectiveness of persistence operations difficult to model. However, we would argue that doctrinal shifts necessary for combating CEIO more effectively are similar to those already underway in the US defence community (such as the focus on 'campaigning' that proceeds according to internal logics rather than generalisable assumptions)[96] and around hot conflicts like the war in Ukraine (e.g. the acknowledgement that capabilities development and deployment should stem from iterative bottom-up learning structures and cultures focused on diverse threat types in the context of national strategic priorities).[97] As a result, though we have made a critique of some prevailing thinking about digital conflict as siloed around unhelpful core assumptions about operational and strategic foundations, we see our clarifications here as fundamentally compatible with existing intellectual-institutional perspectives.

Christopher Whyte, PhD. (cewhyte@vcu.edu) is Associate Professor of Homeland Security and Emergency Preparedness at the L. Douglas Wilder School of Government & Public Affairs at Virginia Commonwealth University. He is author of nearly

[94] Max Smeets, 'US cyber strategy of persistent engagement & defend forward: Implications for the alliance and intelligence collection', *Intelligence and National Security*, 35:3 (2020), pp. 444–53.

[95] Fischerkeller et al., *Cyber Persistence Theory*.

[96] Thomas F. Lynch III, 'Cyberspace: Great power competition in a fragmenting domain', *Orbis*, 68:4 (2024), pp. 607–623

[97] Seth G. Jones, Riley McCabe, and Alexander Palmer, *Ukrainian Innovation in a War of Attrition*, Center for Strategic and International Studies (CSIS) (2023).

https://doi.org/10.1017/eis.2025.10016 Published online by Cambridge University Press

four dozen peer-reviewed research articles, numerous reports, and five books focused on information warfare, the decision-making dimensions of cyber conflict, and the dynamics of organizational innovation and technology adoption.

Ugochukwu Etudo, Ph.D. (etudouo@vcu.edu) is Assistant Professor of Information Systems at Virginia Commonwealth University's School of Business. Prior to this appointment, Ugo was Assistant Professor of Information Systems at the University of Connecticut. Ugo received his PhD from VCU in 2017. His research is focused both on basic inquiry into deep learning models that artificial intelligence in the natural language domain and on the applications of those models to understand maladaptive uses of online social platforms at scale. Ugo's work has appeared in numerous outlets such as Decision Support Systems, Journal of Cybersecurity, Journal of the Association for Information Systems and Information Systems Research.

Cite this article: Christopher Whyte and Ugochukwu Etudo, 'Finding the thieves amongst the liars: Thinking clearly about cyber-enabled influence operations', *European Journal of International Security* (2025), pp. 1–19. https://doi.org/10.1017/eis.2025.10016