Moving Beyond Cyber-Enabled Influence Operations

Michael Genkin[1]

The emergence of the internet and the rise of cyberspace have led to the development of new methods of projecting power and exerting strategic influence, one of which is offensive cyber operations. This article examines the use of offensive cyber for influence operations in incidents in two case studies in Israel and Albania, which were attributed to Iran. The article includes a theoretical analysis of key concepts in offensive cyber operations and influence operations through cyberspace. It shows how ransomware operations can be used to convey messages that are exploited as part of influence operations. Albania countered the attack with a strong diplomatic response, along with international cooperation to attempt to deter future attacks, while the Israeli case demonstrated a novel method of increasing cyber resilience against offensive cyber-enabled influence operations.

With the advent of the internet, a global network of networks, and its subsequent proliferation,[2] it has become a staple of the modern information environment[3] and has enabled the rise of cyberspace.[4] Before long, international actors recognized the centrality of cyberspace in the information environment, its economic significance, and its importance for the generation and exercise of state power.[5] In pursuit of their political and strategic goals, these actors seek to exploit all sources of national power to influence each other's affairs and decision-making, leading to the development of new and novel methods to use cyberspace for

[1] Michael Genkin is a visiting research fellow at King's College London War Studies and a member of the OCWG College of Experts.
[2] Ani Petrosyan, "Internet and Social Media Users in the World 2024," Statista, January 31, 2024, https://www.statista.com/statistics/617136/digital-population-worldwide/.
[3] Ahmad Alzubi, "The Evolving Relationship between Digital and Conventional Media: A Study of Media Consumption Habits in the Digital Era," *THE PROGRESS: A Journal of Multidisciplinary Studies* 4, no. 3 (September 30, 2023): 1–13, https://hnpublisher.com/ojs/index.php/TP/article/view/25.
[4] Marco Mayer et al., "How Would You Define Cyberspace," *First Draft Pisa* 19 (2014): 2014.
[5] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (University of Nebraska Press, 2011), https://doi.org/10.2307/j.ctt1djmhj1; William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, (September 1, 2010), https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain; Tomáš Minárik, "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit," NATO CCDCOE, 2016, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/.

generating influence.[6] But while focusing on certain attributes of cyberspace, which make it conductive to influence operations,[7] and the exploitation thereof to exert influence, some forms of projecting power in cyberspace have received less attention than warranted. One such form is offensive cyber operations (OCOs).[8] As OCOs, and specifically ransomware attacks, are prevalent,[9] this article strives to address this literature gap and examine how OCOs are used in, and in support of, influence operations.

To address the use of ransomware incidents in influence operations and in support of them, this article describes an analytical framework for analyzing such operations, describes ransomware incidents as an example of OCO within the laid-out analytical framework, and provides two case studies demonstrating this form of cyberspace exploitation for influence operations.

Influence Operations in and Through Cyberspace

Influence operations are activities that occur in and through the information environment to affect the attitudes, behaviors, and decision-making of a targeted audience, as well as to advance the objectives of the perpetrator, without the use of force. Operationally, influence operations take place between the originator and the target and follow a sequence of preparation, execution, and exploitation

---

[6] See, for example, Marie Baezner and Sean Cordey, "Influence Operations and Other Conflict Trends," in *Cyber Security Politics* (Routledge, 2022), 17–31; Pascal Brangetto and Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," in *2016 8th International Conference on Cyber Conflict (CyCon)* (IEEE, 2016), 113–26, https://doi.org/10.1109/cycon.2016.7529430; Sean Cordey, "Cyber Influence Operations: An Overview and Comparative Analysis," (ETH Zurich, October 31, 2019), https://doi.org/10.3929/ETHZ-B-000382358; Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations," in *The Oxford Handbook of Cyber Security*, ed. Paul Cornish (Oxford University Press, 2021), 250–272, https://doi.org/10.1093/oxfordhb/9780198800682.013.15; Peter Pijpers and P.A.L. Ducheine, "Influence Operations in Cyberspace – How They Really Work," Amsterdam Law School Legal Studies Research paper No. 2020-61, *Amsterdam Center of International Law*, 2020-31 (2020), https://doi.org/10.2139/ssrn.3698642.

[7] Used interchangeably with information operations in this article, as well in the wider literature.

[8] Offensive cyberspace operations are mainly military, activities in cyberspace designed to deny, degrade, disrupt, destroy, or manipulate in order to achieve denial effects in physical domains. See US Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," US Department of Defense, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[9] On the prevalence of OCOs, see Jakob Bund et al., "EuRepoC Cyber Conflict Briefing – 2023 Cyber Activity Balance," European Repository of Cyber Incidents, January 31, 2024, https://eurepoc.eu/wp-content/uploads/2024/01/EuRepoC-Cyber-Conflict-Briefing-2023-Cyber-Activity-Balance.pdf. On the prevalence of ransomware incidents see, among others, C. David Hylender et al., "Verizon 2023 Data Breach Investigations Report," The Verizon DBIR Team, 2023, https://verizon.com/dbir/; Ani Petrosyan, "Global Firms Targeted by Ransomware 2023," Statista, March 28, 2024, https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/; "The State of Ransomware 2023," Sophos, May 2023, https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf; "The 2024 Crypto Crime Report," Chainalysis, February 2024, https://go.chainalysis.com/rs/503-FAP-074/images/The%202024%20Crypto%20Crime%20Report.pdf.

of successful activities. The preparation stage consists of formulating an intent and selecting a proper strategic narrative. This narrative is a construct that describes a shared, desired objective for the future between the originator and the target and is then operationalized by breaking it down into frames.[10] These frames are designed to exploit the target audience's heuristics and influence the target toward making predetermined decisions. In the execution phase, the prepared frames are injected into the information environment by engaging directly with the target audience or through mediators.[11] Successfully executed activities are exploited, such as by using marketing to amplify the injected narratives, or by selecting new targets whose exploitation would increase the perceived legitimacy of the narrative.[12] "Success" is achieved when the target information environment is shaped in a way that leads the target to change their behavior, or political goals to align favorably with the originator's intent.

Cyberspace is often conceptualized in terms of three layers: the physical network, the logical layer, and the virtual persona. The physical network layer of cyberspace consists of geographic components as well as network components and the physical connections between these components. It forms a highly interconnected network of sometimes overlapping networks, which serves as the medium where cyberspace data travels. The logical layer encompasses non-tangible elements manifested in data or code ("zeros and ones") that are abstracted from the physical network layer, meaning their form or relationships are not tied to individual specific paths or nodes, such as operating systems, protocols, applications, and other software and data components. The virtual persona layer represents an even higher level of abstraction of the logical layer in cyberspace. It uses the rules that apply in the logical layer to create a digital representation of an individual's or entity's identity in cyberspace. This allows real persons or organizations to access the logical level of cyberspace via identifiers such as email addresses or accounts on social media platforms. The identities in the virtual persona layer can significantly diverge from those within the physical domain as individuals and states can alter their attributes by manipulating the logical and physical network layers by using "anonymization" technologies such as the TOR network.[13] The logical layer and the virtual persona layer together constitute the

[10] George Lakoff, "Chapter 1," in *The Political Mind: A Cognitive Scientist's Guide to Your Brain and Its Politics* (Penguin, 2008), 22.
[11] Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations"; Pijpers and Ducheine, "Influence Operations in Cyberspace – How They Really Work."
[12] Robert B Cialdini, "Social Proof: Truths Are Us," in *Influence: The Psychology of Persuasion*, vol. 55 (Collins New York, 2007), 114.
[13] Roger Dingledine, Nick Mathewson, and Paul Syverson, "Tor: The Second-Generation Onion Router," in *In Proceedings of the 13th Usenix Security Symposium*, 2004, https://doi.org/10.21236/ADA465464.

virtual dimension of cyberspace, which overlaps with the virtual dimension of the information environment.

When discussing cyber-enabled influence operations, or cyber operations in support of influence operations, it is tempting to focus solely on the virtual dimension of the information environment. The value of the logical layer of cyberspace for influence operations is straightforward. This layer represents the information stored in cyberspace, which cyber-enabled influence operations aim to exploit by damaging the confidentiality or integrity thereof.[14] These operations are meant to sow confusion and erode civilians' trust in the government by making information that was not meant for public consumption available and drawing attention disproportional to its importance.

Exploiting the virtual persona layer presents another opportunity for influence operations. This exploitation allows precise targeting and direct communication with the target audience, enabling the originator to inject his frames bypassing traditional media moderation and filters. Social media is often abused in this manner, as it allows unlimited dissemination of messaging without limitations of resources and makes messages seem more prominent than they naturally are. This, in turn, can result in lending credibility to the message, leveraging the cognitive bias of compatibility or social proof,[15] and multiplying its effectiveness. The amplified messages can generate influence on themselves,[16] representing examples of influence operations that can be conducted entirely in the virtual

[14] Sometimes also referred to as "doxing," "doxfare" or "hack and leak"—when the leaked information is known to have been previously stolen through a hacking incident. See, for example, Baezner and Cordey, "Influence Operations and Other Conflict Trends"; Brangetto and Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations"; Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations"; Pijpers and Ducheine, "Influence Operations in Cyberspace – How They Really Work." For examples of successful exploitation of damaging data integrity or confidentiality for influence, see Nikolay Koval, "Revolution Hacking," *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (2015), 55–65, https://www.ccdcoe.org/uploads/2018/10/Ch06_CyberWarinPerspective_Koval.pdf; Heidi Moore and Dan Roberts, "AP Twitter Hack Causes Panic on Wall Street and Sends Dow Plunging," *The Guardian*, April 23, 2013, https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall.

[15] Cialdini, "Social Proof: Truths Are Us."

[16] For examples of such messaging, including disinformation and trolling, see Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* 31, no. 2 (May 2017): 211–236, https://doi.org/10.1257/jep.31.2.211; Alexander Lanoszka, "Disinformation in International Politics," *European Journal of International Security* 4, no. 2 (June 2019): 227–248, https://doi.org/10.1017/eis.2019.6; Robert S. Mueller III, "Report on the Investigation Into Russian Interference in the 2016 Presidential Election. Volumes I & II.(Redacted Version of 4/18/2019)," 2019; J.-B. Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies," report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

persona layer. Alternatively, they can exploit the virtual persona layer to capitalize on successful cyber operations that occurred in the logical layer.[17]

In the general case, the attraction of cyberspace for executing influence operations can be explained by the observation that most of the cyber operations performed in support of influence operations are relatively non-sophisticated[18] and thus can be executed while incurring very low costs.[19] In addition, due to the inherent technical anonymity of cyberspace and the lack of mature legal frameworks, there is little chance of technical attribution,[20] which might carry a risk of escalation or counter measures.

Interestingly, it appears that while some of the often-quoted case studies—such as DDoS attacks—technically represent attacks against the physical network layer of cyberspace, the literature on cyber-enabled influence operations chooses to focus on how those attacks can be used to exploit the virtual dimension. This choice is made possible due to the effect mechanisms that the above-mentioned cases utilize through the virtual dimension and specifically through the logical layer of cyberspace. Another possible explanation for this choice might be the belief that attacks that exploit the physical network layer lack the capability to inject narrative frames and thus are not useful in influence operations. One interesting outlier to this trend is a recent work by Dolev and Siman-Tov that examined a series of ransomware incidents in Israel which were attributed to Iranian-nexus threat actors. They noted that the behavior exhibited during those incidents did not coincide with the financial motivation that is typical with ransomware incidents but resembled that of an influence operation.[21] This article builds upon this premise and expands it to a study of the applicability of effects through the physical network layer of cyberspace for, and in support of, influence operations.

---

[17] Pijpers and Ducheine, "Influence Operations in Cyberspace – How They Really Work."
[18] At least from the purely technical implementation point of view.
[19] Baezner and Cordey, "Influence Operations and Other Conflict Trends"; Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations"; Max Smeets, "The Strategic Promise of Offensive Cyber Operations," 2018.
[20] Clara Assumpção, "The Problem of Cyber Attribution Between States," E-International Relations (blog), May 6, 2020, https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/; Florian J. Egloff, "Contested Public Attributions of Cyber Incidents and the Role of Academia," *Contemporary Security Policy* 41, no. 1 (January 2, 2020): 55–81, https://doi.org/10.1080/13523260.2019.1677324; Oliver Fitton, "Cyber Operations and Gray Zones: Challenges for NATO," *Connections* 15, no. 2 (2016): 109–19, https://www.jstor.org/stable/26326443; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.
[21] Boaz Dolev and David Siman-Tov, "Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks," INSS Special Publication, January 27, 2022, https://www.inss.org.il/publication/cyber-iran/.

Ransomware as a Medium of Influence

Ransomware is a subset of malware designed to damage the availability of data by restricting access to it until a requested ransom amount from the attacker is satisfied.[22] Not content with simply deploying malware and hoping the victim will comply with the ransom demand,[23] the threat actors perpetrating those incidents innovated in two significant ways. One was by shifting to "locker ransomware," which renders the system non-functional by displaying a "ransom note" until the ransom is paid, thus disrupting the availability of the affected system as well and creating a messaging opportunity that is hard to ignore. The second was by moving to "double extortion" tactics where the threat actor damages the confidentiality of the victim's data by exfiltrating it before restricting access, thus creating an additional incentive for the victim to pay the ransom unless the data would be leaked to the public.[24] This evolution makes ransomware a potentially interesting tool to employ in influence operations, as the "locker ransomware" provides an opportunity to exploit the logical layer of cyberspace to inject an influence frame into the targeted information environment, while denying the target the ability to avoid the injected frame due to the disruption caused on the physical network layer of cyberspace. Finally, through their disruptive effects in cyberspace, well-designed ransomware incidents might also generate denial effects in the physical domain.[25] Due to the disruption caused on the logical and physical network layers through damaging system and data availability, and the possible denial effects through cyberspace, ransomware attacks can be considered a form of OCOs. Combining "locker ransomware" with "double

[22] Amin Kharraz et al., "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, ed. Magnus Almgren, Vincenzo Gulisano, and Federico Maggi, vol. 9148, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2015), 3–24, https://doi.org/10.1007/978-3-319-20550-2_1.

[23] Early ransomware attacks opted to restrict access to data only, leaving the system itself functional but causing the victims to be unaware of the incident taking place until they attempted to use the ransomed data. Additionally, victims of such incidents might also have a backup of the data and resort to restoring it from the backup rather than pay the ransom.

[24] Catalin Cimpanu, "Reveton Ransomware Distributor Sentenced to Six Years in Prison in the UK," ZDNet, April 9, 2019, https://www.zdnet.com/article/reveton-ransomware-distributor-sentenced-to-six-years-in-prison-in-the-uk/; Kevin Savage, Peter Coogan, and Hon Lau, "The Evolution of Ransomware," August 6, 2015, https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf.

[25] Sara Morrison, "The Chaotic and Cinematic MGM Casino Hack, Explained," Vox, September 15, 2023, https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware; Jack Beerman et al., "A Review of Colonial Pipeline Ransomware Attack," in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 2023, 8–15, https://doi.org/10.1109/CCGridW59191.2023.00017; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; Ax Sharma, "BlackCat (ALPHV) Claims Swissport Ransomware Attack, Leaks Data," BleepingComputer (blog), February 15, 2022, https://www.bleepingcomputer.com/news/security/blackcat-alphv-claims-swissport-ransomware-attack-leaks-data/.

extortion" tactics takes this even further allowing both an additional messaging channel, as well as cover, which might improve the ability to effectively exploit, what would otherwise be a classic hack-and-leak operation. Ransomware also offers an interesting case showing uncoordinated, or loosely coordinated, actors who are able to achieve effects that might amount to those of an influence operation in shifting policy priorities due to cumulative, second- and higher-order effects such as undermining citizens' trust in government services or causing a diversion of resources.[26]

Armed with an understanding of ransomware incidents as a form of OCO and an analytical framework for assessing influence operations, this article now proceeds by applying the presented analytical framework to two case studies—the July 2022 e-Albania ransomware incident and the 2022–2023 "BlackShadow" campaign against Israel.

Case Study #1: The e-Albania Ransomware Incident

On July 15th, 2022, just before the World Summit of Free Iran—an event affiliated with Mujahedeen-e-Khalq (MEK)[27] that was planned to take place at the end of July near the Albanian city of Durres—the Albanian National Agency of Information Society (AKSHI) was attacked by a threat actor calling himself "HomeLand Justice," purporting to be an Albanian group opposed to the government's support of the MEK. The incident involved the deployment of ransomware that caused disruption to the e-Albania portal, as well as multiple websites and services of the Albanian government. In a later statement the prime minster of Albania claimed that the aim of this cyberattack was to paralyze public services, erase digital systems, hack into state records, steal government intranet electronic communications, and stir chaos and insecurity in the country.[28]

To help mitigate the attack the Albanian government enlisted the support of its NATO ally—the United States—in the form of the FBI and US Cyber Command personnel who were deployed to assist with forensic investigations and perform a "hunt forward" mission in the Albanian networks, respectively. In addition, they turned to the private sector, specifically the Microsoft DART and Mandiant incident

[26] Jamie MacColl et al., "The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society," RUSI, January 2024, https://static.rusi.org/ransomware-harms-op-january-2024.pdf.
[27] People's Mujahedeen Organization of Iran is an Iranian opposition organization based in Albania, posing as a future government-in-exile.
[28] "Videomessage of Prime Minister Edi Rama," Albanian Government Council of Ministers, September 7, 2022, https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama/; Luke Jenkins et al., "ROADSWEEP Ransomware Targets the Albanian Government," Mandiant, August 4, 2022, https://www.mandiant.com/resources/blog/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against.

response teams.[29] At the center of the incident was a disruption caused by a new ransomware malware, which was used to display a political message on the encrypted systems—"Why should our taxes be spent on the benefit of DURRES terrorists?"—followed by an extensive social media campaign based on materials that were exfiltrated from the AKSHI networks prior to the disruptive phase of the attack. As a result of its investigation, Microsoft DART was able to attribute the "HomeLand Justice" threat actor to the Iranian Ministry of Intelligence and Security (MOIS), based on forensic artifacts and prior public attribution. This attribution was echoed by Albanian Prime Minister Edi Rama, who stated that "the July cyberattack was carried out by multiple hacker groups linked to the Islamic Republic. Four groups were identified, one of which was a notorious international cyber-terrorist group with a history of targeting countries like Israel or Saudi Arabia."[30.]

Following the July cyberattack, on September 7th, 2022, the Albanian government issued an unprecedentedly strong reaction by formally attributing the attack to the Iranian state. They announced the severance of all diplomatic ties with Iran and ordered the Iranian diplomatic staff in Albania to leave the country within 24 hours.[31] The Albanian response was followed by statements of support from the United Kingdom, NATO, the European Union, and the United States[32] Furthermore,

---

[29] Cyber & Infrastructure Security Agency, "Iranian State Actors Conduct Cyber Operations Against the Government of Albania," September 23, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a; Cyber National Mission Force Public Affairs, "'Committed Partners in Cyberspace': Following Cyberattack, US Conducts First Defensive Hunt Operation in Albania," U.S. Cyber Command, March 23, 2023, https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/; Jenkins et al., "ROADSWEEP Ransomware Targets the Albanian Government"; Microsoft Threat Intelligence, "Microsoft Investigates Iranian Attacks against the Albanian Government," Microsoft Security Blog, September 8, 2022, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/.

[30] "Videomessage of Prime Minister Edi Rama."

[31] Florion Goga et al., "Albania Cuts Iran Ties over Cyberattack, U.S. Vows Further Action," Reuters, September 7, 2022, https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/; "Videomessage of Prime Minister Edi Rama."

[32] Council of the EU, "Cyber-Attacks: Declaration by the High Representative on Behalf of the European Union Expressing Solidarity with Albania and Concern Following the July Malicious Cyber Activities" (Council of the EU, September 8, 2022), https://www.consilium.europa.eu/en/press/press-releases/2022/09/08/cyber-attacks-declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-albania-and-concern-following-the-july-malicious-cyber-activities/; Foreign, Commonwealth & Development Office and The Rt Hon James Cleverly MP, "UK Condemns Iran for Reckless Cyber Attack against Albania" (GOV.UK, September 7, 2022), https://www.gov.uk/government/news/uk-condemns-iran-for-reckless-cyber-attack-against-albania; NATO, "Statement by the North Atlantic Council Concerning the Malicious Cyber Activities against Albania" (NATO, September 8, 2022), https://www.nato.int/cps/en/natohq/official_texts_207156.htm; The White House, "Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania," September 7, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/.

the US Department of the Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions on MOIS and on the Minister of Intelligence, Esmail Khatib, by freezing their assets.[33]

Analyzing this sequence of cyberattacks against Albania as an influence operation we can easily discern the following: While we cannot fully know the strategic intent of this influence operation, the chosen frames used both in the message presented by the ransomware[34] and the following social media exploitation[35] claimed to protest "government corruption" and "support of terror," with later social media frames including claims that the attack was directed against the government and not Albanian citizens. It is tempting to assume the easy proposition that the strategic goal behind the attack was to deny the MEK the political support of the Albanian government. Another thesis that one might propose is that, as the attack followed a series of attacks against Iran,[36] some of which were attributed to the MEK, the strategic goal was to retaliate as well as establish a deterrent threat coercing the Albanian government to act and limit the ability of the MEK to execute cyberattacks against Iran.[37] Finally, from the target response to the operation—to the diplomatic denouncing—it is clear that the target viewed this operation as harmful.

The Albanian government's response to the attack comprised a series of attempts to gain initiative and deter further attacks. Its initial effort was defensive and aimed to stop further attack activity inside the AKSHI networks and recover service availability. The next stage was to issue a punishment, for which Albania shortly considered invoking Article 5 of the NATO charter,[38] but it finally settled, likely after

[33] U.S. Department of the Treasury Office of Foreign Assets Control, "Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities" (U.S. Department of the Treasury, September 9, 2022), https://home.treasury.gov/news/press-releases/jy0941; A. J. Vicens, "U.S. Sanctions Iranian Ministry of Intelligence in Response to Albanian Cyberattack," CyberScoop (blog), September 9, 2022, https://cyberscoop.com/microsoft-albania-iran-cyberattack/.
[34] Jenkins et al., "Roadsweep Ransomware Targets the Albanian Government."
[35] Microsoft Threat Intelligence, "Microsoft Investigates Iranian Attacks against the Albanian Government."
[36] This thesis, as well as some following analysis, assumes that the political attribution of the attack made by Edi Rama in his "Videomessage of Prime Minister Edi Rama" to be correct.
[37] the grugq, "Albanian Cyber War," Substack newsletter, The Info Op (blog), September 7, 2022, https://grugq.substack.com/p/albanian-cyber-war; Mahmoud Hakam, "Major Cyber Attack on Tehran's Islamic Culture & Relations Organization," Iran News Update (blog), July 4, 2022, https://irannewsupdate.com/news/iranian-opposition/major-cyber-attack-on-tehrans-islamic-culture-relations-organization/; AP News, "Iran Exiles Claim Disrupting Tehran's Surveillance Cameras," AP News, June 2, 2022, https://apnews.com/article/politics-iran-middle-east-dubai-united-arab-emirates-f9b79784cba77adcf8c88dafde11ee84; A. J. Vicens, "Deep Dive into Hack against Iranian State TV Yields Wiper Malware, Other Custom Tools," CyberScoop (blog), February 18, 2022, https://cyberscoop.com/iran-state-tv-hack-predatory-sparrow-indra/.
[38] Maggie Miller, "Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack," Politico (blog), October 5, 2022, https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347.

achieving significant enough technical attribution of the originator,[39] on an exceptionally strong direct diplomatic response combined with economic sanctions applied by the US Treasury Department against the suspected attackers. The subsequent September 2022 attack by "HomeLand Justice" against the TIMS system showed that, albeit considered strong, the Albanian response was not enough to deter further attacks.

Operationally, the e-Albania incident utilized software—specifically ransomware malware—to disrupt entities and services at the physical network, logical, and virtual persona levels of cyberspace, making this incident an OCO. From the vantage point of an influence operation, during the e-Albania incident the originator exploited the logical layer for injecting their narrative frames and tried to exploit the virtual persona layer as well, albeit without any visible evidence of successful exploitation. In addition to the injection of frames, the originator exploited the logical layer to exfiltrate sensitive information—to be leaked at later stages of the influence operation—but again, at least as far as visible evidence shows, failed to exploit and capitalize on.

Case Study #2: 2020–2023 "BlackShadow" Campaign Against Israel

The focus of the second case study is a series of attacks by a self-proclaimed cybercrime group called "BlackShadow," which began in December 2020 and was ongoing as of December 2023. The first incident involving "BlackShadow" targeted the Israeli insurance company Shirbit and was not a ransomware attack but rather a hack-and-leak incident.[40] It lacked specific narrative frames and can only be considered an influence operation in the most rudimentary sense of undermining public confidence in the state and sowing chaos.[41] As the incident came to light, Shirbit representatives claimed that it was a cyberterrorism attack against Israel and not financially motivated. This claim was further corroborated by a report from an Israeli cybersecurity company, ClearSky, which was leaked by an Israeli financial magazine.[42] The ClearSky report suggested a possible connection to Iran

---

[40] Tzvi Joffre, "Government to Reconsider Using Shirbit Insurance After Large Cyberattack," *Jerusalem Post*, December 7, 2020, https://www.jpost.com/israel-news/government-to-reconsider-using-shirbit-insurance-after-large-cyberattack-651382.

[41] Brangetto and Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations"; Koval, "Revolution Hacking"; Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations."

[42] Amitai Ziv, "Cyber Attack on Shirbit—Who Is Behind It and Why?" [in Hebrew] *TheMarker*, December 4, 2020, https://www.themarker.com/technation/2020-12-04/ty-article/.premium/0000017f-db42-df9c-a17f-ff5a9c540000?lts=1713292167615; "1.12 סקירת אירוע סייבר בחברת שירביט" (Tel Aviv, Israel: ClearSky Cyber Security, December 1, 2020), https://img.haarets.co.il/bs/0000017f-db52-d856-a37f-ffd215bd0000/cd/b5/edfbba34893bebc024fc4a688593/20201204-101626.pdf.

or OpIsrael,[43] based on the use of the corresponding hashtag in the initial "BlackShadow" social media messaging and the acquiring of what it assumed, with medium confidence, to be the malware used during the incident. Other cybersecurity companies later attributed this malware to an Iranian-nexus activity due to technical and operational similarities.[44] While the threat actor claimed the attack was financially motivated, their tactics went beyond the usual techniques employed by ransomware actors to pressure victims into paying the ransom, including directly contacting media outlets and publishing parts of the negotiation correspondence.[45] This unusual conduct led Shirbit to claim the incident as an "act of cyber-terrorism," although the Israeli state security and cybersecurity agencies had minimal involvement, limited to acknowledging the attack and publishing some revised cyber-hygiene guidelines for Israeli companies by the Israel National Cyber Directorate (INCD).[46]

Following the appearance of "BlackShadow" in the Shirbit incident, the threat actor proceeded to conduct additional hack-and-leak operations against Israeli targets, which failed to generate significant media attention. In August 2021, "BlackShadow" introduced a new tactic by utilizing ransomware against an Israeli target for the first time in an incident involving Bar-Ilan University.[47] While this attack did not receive much media attention, reports claimed the involvement of the INCD and the Israeli security services in responding to the incident. Similar to previous "BlackShadow" victims, Bar-Ilan University claimed that the incident was a cyberterrorism event and blamed Iran for it. Interestingly, while the Israeli

[43] OpIsrael is an annual coordinated cyber-attack where hacktivists attack Israeli government and even private websites with DDoS attacks and more David Shamah, "As Cyber-War Begins, Israeli Hackers Hit Back," *The Times of Israel* (blog), April 7, 2013, http://www.timesofisrael.com/as-cyber-war-begins-israeli-hackers-hit-back/.

[44] Amitai Ben Shushan Ehrlich, "From Wiper to Ransomware: The Evolution of Agrius," SentinelOne LABS, May 25, 2021, https://assets.sentinelone.com/sentinellabs22/evol-agrius; "An In-Depth Look at APT33," CyberWarCon, 2019.

[45] Dolev and Siman-Tov, "Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks."

[46] INCD Spokesperson, "Data Breach Event at Shirbit," Israel National Cyber Directorate, December 1, 2020, https://www.gov.il/en/pages/news_shirbit.

[47] Amitai Ben Shushan Ehrlich, "New Version of Apostle Ransomware Reemerges in Targeted Attack on Higher Education," SentinelOne (blog), September 30, 2021, https://www.sentinelone.com/labs/new-version-of-apostle-ransomware-reemerges-in-targeted-attack-on-higher-education/; "Mass Data Leak after Bar Ilan University Refuses to Pay Hacker $2.5m," *Times of Israel* (blog), September 9, 2021, https://www.timesofisrael.com/liveblog_entry/mass-data-leak-after-bar-ilan-university-refuses-to-pay-hacker-2-5m/; Amitai Ziv, "Cyberattack Hits Israel's Bar Ilan University: 'Data Is Being Erased Right Now,'" *Haaretz*, August 15, 2021, https://www.haaretz.com/israel-news/tech-news/2021-08-15/ty-article/.premium/cyberattack-on-israeli-university-data-being-erased-right-now/0000017f-e396-d75c-a7ff-ff9ff65a0000; Amitai Ziv, "Does Crime Pay? A Conversation with a Hacker Targeting Israel," *Haaretz*, September 1, 2021, https://www.haaretz.com/israel-news/tech-news/2021-09-01/ty-article/.premium/does-crime-pay-a-conversation-with-a-hacker-targeting-israel/0000017f-f15d-dc28-a17f-fd7f7f3d0000.

security services remained silent about the attribution, Dolev and Siman-Tov[48] echoed this claim based on their familiarity with the response effort during the "BlackShadow" incidents. They noted that the conduct of the threat actor was not typical of a ransomware operation but included "trash-talking" the negotiators and simplistic political messaging in broken English, indicating a motive different from extorting ransomware payment.

After the Bar-Ilan University incident, the "BlackShadow" threat actor continued to target Israeli entities, such as the diamond industry in March 2022,[49] and the tech and education sectors through 2023.[50] These attacks involved wiper and ransomware operations but, again, failed to generate significant public attention. Ultimately, in October 2023, another threat actor—calling itself "Malek Team"—appeared, executing a technically successful hack-and-leak operation against the Ono Academic College, leaking multiple items of personally identifiable and sensitive information, and causing some interference with the college services.[51] Later, in December 2023, the same actor executed a hack-and-leak operation against Ziv Medical Center, again leaking a myriad of private and sensitive information, but with no evidence of disrupting the functioning of the medical center.[52] Following this incident, the INCD swiftly attributed it and the "Malek Team" threat actor to the Iranian government and specifically to the same actor as "BlackShadow." In addition, in a first, the attribution statement explains that the deviation from the regular "BlackShadow" modus operandi of disrupting their

[48] Dolev and Siman-Tov, "Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks."
[49] Adam Burgher, "Fantasy – a New Agrius Wiper Deployed through a Supply-Chain Attack," WeLiveSecurity (blog), September 7, 2022, https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/.
[50] Or Chechik et al., "Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors," Unit 42 (blog), November 6, 2023, https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/; Marc Salinas Fernandez and Jiri Vinopal, "Agrius Deploys Moneybird in Targeted Attacks Against Israeli Organizations," Check Point Research (blog), May 24, 2023, https://research.checkpoint.com/2023/agrius-deploys-moneybird-in-targeted-attacks-against-israeli-organizations/; Bill Toulas, "Iranian Hackers Use New Moneybird Ransomware to Attack Israeli Orgs," BleepingComputer (blog), May 24, 2023, https://www.bleepingcomputer.com/news/security/iranian-hackers-use-new-moneybird-ransomware-to-attack-israeli-orgs/.
[51] Check Point Research, "The Iron Swords War," Check Point Blog (blog), October 18, 2023, https://blog.checkpoint.com/security/the-iron-swords-war-cyber-perspectives-from-the-first-10-days-of-the-war-in-israel/; Ryan Gallagher, "War Tests Israeli Cyber Defenses as Hack Attempts Soar," Bloomberg, October 18, 2023, https://www.bloomberg.com/news/newsletters/2023-10-18/war-tests-israeli-cyber-defenses-as-hack-attempts-soar.
[52] Daryna Antoniuk, "Iran-Linked Hackers Claim to Leak Troves of Documents from Israeli Hospital," The Record by Recorded Future (blog), December 4, 2023, https://therecord.media/ziv-hospital-israel-hackers-claim-to-leak-data; Inon Ben Shushan, "Hackers Steal IDF Patient Records from Cyberattack on Israeli Hospital," *Jerusalem Post*, December 3, 2023, https://www.jpost.com/israel-news/defense-news/article-775843; Ministry of Health Spokesperson, "Joint Announcement by Ziv Medical Center, the Ministry of Health and the Israel National Cyber Directorate," Ministry of Health, November 28, 2023, https://www.gov.il/en/pages/27112023-01.

targets by using ransomware or wiper malware in the Ziv Medical Center incident was due to interference from the Israel Security Agency[53] and the Israel Defense Forces, which also participated in the attribution.[54]

Analyzing the "BlackShadow" campaign as an influence operation shows that contrary to the "HomeLand Justice" campaign against Albania, it is harder to discern a specific narrative or strategic intent, as the chosen frames change frequently, sometimes even during the same incident. Such behavior might be in line with a strategic goal of "sowing chaos" or weakening social cohesion by creating civilian distrust in national institutions.[55] Tactically, the "BlackShadow" campaign evolved throughout its duration from a classic cyber-enabled influence operation, taking the form of a series of hack-and-leak incidents, to the deployment of OCO capabilities.

The long-lasting nature of the "BlackShadow" campaign allows for the examination of the evolution of the INCD and Israel's response efforts. Notably, in the incidents that took place from December 2020 to March 2023, the INCD chose to "update" on incidents taking place and extended support to the investigation of the incidents, while emphasizing the role of the private sector in the investigation and response effort.[56] Specifically, it left the attribution effort entirely in the hands of the private sector. This changed significantly with the incidents in October 2023, when the INCD claimed a leading role in the investigation and response to the cyber incidents that were part of the "BlackShadow" campaign, together with other Israeli national-security organizations. Moreover, the INCD chose to publicly and formally attribute those incidents to Iran and even linked the "Malek Team" persona to the "BlackShadow" campaign.[57] One might speculate that some, if not most, of the reasoning behind this change was the securitization of those incidents both by the Israeli public and the threat actor, due to the outbreak of the war

[53] Commonly known as the Shin Bet.
[54] INCD Spokesperson, "Iran and Hezbollah behind an Attempted Cyber Attack on an Israeli Hospital," Israel National Cyber Directorate, December 18, 2023, https://www.gov.il/en/pages/ziv181223.
[55] Brangetto and Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations"; Koval, "Revolution Hacking"; Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations."
[56] Ben Zion Gad, "'Black Shadow' Hackers Leak Data from Israeli LGBT App," *Jerusalem Post*, October 31, 2021, https://www.jpost.com/israel-news/iranian-hackers-breach-israeli-company-cyberserve-683529; INCD Spokesperson, "Data Breach Event at Shirbit"; Tzvi Joffre and Tamar Uriel-Beeri, "Black Shadow Hackers Strike Again, Leak Documents in New Cyberattack," *Jerusalem Post* (blog), March 13, 2021, https://www.jpost.com/jpost-tech/israeli-car-financing-company-hacked-private-information-held-for-ransom-661865; Ziv, "Cyberattack Hits Israel's Bar Ilan University."
[57] INCD Spokesperson, "Iran and Hezbollah behind an Attempted Cyber Attack on an Israeli Hospital"; Ministry of Health Spokesperson, "Joint Announcement by Ziv Medical Center, the Ministry of Health and the Israel National Cyber Directorate"; "קבוצת התקיפה האיראנית Black Shadow," Israel National Cyber Directorate, April 9, 2024, https://www.gov.il/BlobFolder/reports/alert_1727/he/ALERT-CERT-IL-W-1727.pdf.

between Israel and Hamas in the Gaza Strip. In this regard, it is interesting to note that when reporting on the Ziv Medical Center incident, the Israeli press chose to treat it as the "fourth attack against an Israeli hospital,"[58] even though it was the first incident of its kind involving the "BlackShadow" threat actor, while the other incidents were attributed to various actors. As such, the Israeli press demonstrated an example of the cumulative effect of cyber incidents, which, moreover, was caused by loosely, if even, coordinated threat groups.

This provides another possible aspect of the reasoning behind the INCD's decision to take a leading role and formally attribute these incidents to Iran. By formally and visibly attributing those incidents to an enduring rival, it is plausible to assume that the INCD aimed to break the cumulative effect by differentiating between the previous criminal ransomware incident and this incident. In addition, it may have sought to capitalize on a possible "rally around the flag"[59] effect by signaling that the government is successfully handling the response and protecting the people when the attacker is a rival state. This also blunts the influence operation by making the Israeli public wary of the messaging from an enemy state.

Another notable choice by Israeli authorities in response to the "BlackShadow" campaign was the privacy protection regulation and the Privacy Protection Authority to limit the spread of leaked materials.[60] This potentially limits the ability to exploit the virtual persona layer for amplifying the leaks and generates resilience against attempted influence operations.

Discussion and Conclusions

This paper set out to examine whether OCOs, and especially ransomware incidents, play a role in influence operations, and the answer is likely "yes." Specifically, OCOs deny the target from easily brushing off hack-and-leak operations, thus minimizing the significance of an incident by using the coercive

[58] Ben Shushan, "Hackers Steal IDF Patient Records from Cyberattack on Israeli Hospital"; Milàn Czerny, "Start-up Nation? Israel's Cyber Defense Collapsed on October 7 and Iranian Hacker Groups Keep Attacking," Ynetnews, January 22, 2024, https://www.ynetnews.com/business/article/hjynr11jk6; Omer Kabir, "Iran and Hezbollah Were behind Cyberattack on Israeli Hospital, Says National Cyber Directorate," CTech by Calcalist, December 18, 2023, https://www.calcalistech.com/ctechnews/article/h1owft6it.

[59] Shingo Hamanaka, "The Ground Operation Sent Citizens into a Frenzy: The Rally around the Flag Effect during Operation Protective Edge," *Global Security: Health, Science and Policy* 5, no. 1 (2020): 142–52; Alan J Lambert, John P. Schott, and Laura Scherer, "Threat, Politics, and Attitudes: Toward a Greater Understanding of Rally-'round-the-Flag Effects," *Current Directions in Psychological Science* 20, no. 6 (2011): 343–48; Sharon Matzkin, Ryan Shandler, and Daphna Canetti, "The Limits of Cyberattacks in Eroding Political Trust: A Tripartite Survey Experiment," *British Journal of Politics and International Relations*, 2023, 13691481231210383.

[60] Ministry of Health Spokesperson, "Joint Announcement by Ziv Medical Center, the Ministry of Health and the Israel National Cyber Directorate."

nature of the disruption to call attention to an audience. This attention can be—and is—exploited to inject framed messages that serve the narrative and strategic intent of the OCO perpetrator. The cases examined in this article show the versatility of OCOs as an element in the wider scope of influence operations, ranging from furthering specific strategic intents to wider goals such as "sowing chaos." In both cases examined, the target of the influence operation deemed the influence attempt unwelcome, which is not surprising given the coercive nature of OCOs.

The perceived malicious intent of the influence operations analyzed can also be inferred from the significance of the attribution of the operation by both targeted nations and the strong diplomatic response in the Albanian case, which involved denouncing the Iranian state for the attack. While the instruments chosen for responding to the disruption and the influence effects differed in the two cases, both targets emphasized the importance of public-private cooperation in mitigating the disruption and restoring service availability. Additionally, both attributed the operations, with each target giving different weight to the responsibility of the national agencies, based on the strategic context and national capacity, with international cooperation acting as a complement when national capacity was lacking.

This might amount to an alternative rationale for the call to improve cyber resilience, especially vis-à-vis ransomware attacks, but further examination is needed. The unique properties of cyberspace—the ability to exploit vulnerabilities to modify cyberspace itself, the vulnerability-rich nature of cyberspace, and its susceptibility to cumulative effects—mean that restricting an adversary from a single incident or increasing the cost for them is not a viable strategy. It is believed that it is not possible to fully protect a nation against cyberattacks as long as an adversary maintains his initiative and persists in efforts to exploit vulnerabilities. Given enough time, the adversary is bound to succeed in generating enough gains to achieve a strategic level effect and "succeed" in the influence operation. The cases presented offer another approach. The Albanian case proposes a comprehensive strategy involving strong policy, cyber-defense, as well as operational and diplomatic measures to regain initiative and deter the adversary from further activity. In contrast, the Israeli case moves the resilience efforts to the virtual persona level to try to mitigate the possibility of exploiting amplification and multiplication effects, which are characteristic of this level of cyberspace and strive to make OCOs in support of influence operations less attractive.

This study makes several contributions. First, it expands our understanding of using cyberspace for influence operations by introducing OCOs, and specifically

ransomware, as a method of exploiting both the physical network and logical layers of cyberspace for influence operations. Second, it identifies an additional cyberspace vulnerability, resulting from its susceptibility to cumulative effects and the inherent challenges of attribution, which allows for an additional method of amplifying certain narratives in influence operations, potentially at lower costs than initially assumed. Finally, it explores possible policy responses to the exploitation of OCOs for influence operations and proposes that these responses enjoy cumulative effects, similar to other activities in cyberspace. Further work is needed to determine the specific design of responses that could maximize the utility against OCOs used for influence operations.

Acknowledgments

The author thanks A.C. and O.S. for their useful and thoughtful remarks during the brainstorming sessions that led to this work, albeit the planned collaboration failed to materialize due to Hamas's October 7 attack on Israel and the subsequent war that followed.