Special Publication

The Influence-Cybercrime Nexus: How Cybercriminal Infrastructure is Reshaping Authoritarian Operations Against Democracies

Ari Ben-Am and Vera Michlin-Shapir | August 23, 2026

Introduction

In recent years, a considerable effort has been devoted to countering attempts by authoritarian state actors to disseminate manipulated information that undermines liberal democratic institutions and influences domestic audiences. These activities, often referred to as influence operations,[1] have prompted the European Union to go as far as stating that: "Tanks or missiles are no longer the main weapons in attacks on democratic societies. FIMI[2] has become one of the defining security and foreign policy challenges of the 2020s, alongside other hybrid threats."[3] While most research and literature has focused on the narratives, content, and online networks that comprise influence operations, much less attention has been given to the underlying cyber infrastructure that enables them — infrastructure that is often provided by cybercriminals.

State agencies and private cybersecurity firms recognize that cybercriminal activity, particularly ransomware, poses a threat to national security. The UK's National Crime Agency (NCA) observes that: "The deployment of ransomware remains the greatest serious and organized cybercrime threat to the UK, threatening Critical National Infrastructure and posing a risk to national security."[4] However, most national security agencies relegate cybercrime to

---

[1] See, for example, Gavin Wilde, "SCOTCH: A Framework for Rapidly Assessing Influence Operations," Atlantic Council, May 24, 2021; National Security and Intelligence Committee of Parliamentarians, "Special Report on Foreign Interference," 2024; European Commission, "Action Plan Against Disinformation," 2018.

[2] The European External Action Service (EEAS) developed the framework of Foreign Information Manipulation and Interference (FIMI) to conceptualise, assess, and counter such threats.

[3] EUvsDisinfo, "Foreign Information Manipulation and Interference (FIMI) Explained," March 15, 2026.

[4] National Crime Agency (UK), "Cybercrime," n.d.

law enforcement bodies, and cybercrime is not considered a multifaceted threat to national security for states globally. Most importantly, cybercrime is not seen as a key enabler of other hostile activity targeting Western states, namely cyber-attacks on critical infrastructure and influence operations.

This paper argues that the growing centrality and integration of cybercriminal infrastructure within authoritarian state actors' influence efforts to undermine and subvert liberal democracies represents a significant and underappreciated threat. Throughout this paper, the term 'influence operations' is used as shorthand for adversarial geopolitical online influence operations. These campaigns consist of coordinated, inauthentic online activities at the tactical level, sustained by state-linked or state-like bureaucratic structures that render them methodical and persistent. Their strategic objective is to manipulate target audiences in ways that erode the national security of the targeted states. This paper refers to cybercrime as a scope of activities primarily motivated by illicit financial gain and personal profit that includes cyber-dependent crime, such as illegal access to systems, interference with or interception of data or system functions and the distribution of tools used to commit these offenses, and cyber-enabled crime (forgery, theft, fraud and money laundering).[5]

The increased centrality of cybercriminal activities to nation-state cyber operations has been apparent for years. In February 2025, Google Threat Intelligence published research showing how online criminal marketplaces serve as hubs for selling leaked data, infostealer logs, malware, initial access, and other illicit services that not only pose direct threats to national security, but also enable nation-state threat actor groups to promote their own interests, including espionage and financial gain.[6] While the relationship between cybercrime and cyber operations is apparent, cyber operations are not the sole uses of cybercrime resources by authoritarian state actors in services of promoting their national interests. The growing use of influence operations online, and their overlap and operational fusion with cyber and kinetic operations, has led authoritarian adversaries to make greater use of cybercriminal services and resources in support of influence operations. This is a logical progression for multiple reasons.

Firstly, the cybercriminal underground offers distinct advantages for influence operations, which aspire to be covert while simultaneously operating highly overtly, and have a different risk calculus for attribution and exposure than cyber operations and espionage. Exposure is not necessarily a bad thing; however, when it is, the use of criminal services and infrastructure provides an additional degree of separation and plausible deniability.

Secondly, online influence operations are still a comparatively small portion of the total expenditure of nation-states and their defense apparatuses, at least when compared to cyber

---

[5] The definition relies on criminalization criteria outlined in the UN Convention Against Cybercrime; see United Nations Office on Drugs and Crime, "United Nations Convention Against Cybercrime," n.d. Unlike the UN convention, we refer to cybercrime as activity with a clear for-profit intent.

[6] Google Threat Intelligence Group, "Cybercrime: A Multifaceted National Security Threat," Google Cloud, February 11, 2025.

operations or other intelligence disciplines. The criminal underground, which exists independently of the nation-state and is not reliant on it, can provide cost-effective services which would be expensive or difficult to otherwise develop. This is particularly useful in an era of increased geopolitical competition, when states seek to conduct adverse activities at scale.

This paper makes several original contributions. First, it develops the concept of cybercriminal infrastructure, defining it as a broad set of foundational tools, functions, and services. It questions current approaches and methods of countering information operations. Second, by incorporating the critical role that cybercriminals play in the complex ecosystems of demand, supply, and technological enablement of influence operations, it reconceptualizes understandings of the dynamics that fuel these operations. Finally, it advances a set of operational recommendations that suggest a market-disruption approach to countering influence operations, shifting the focus away from social network dynamics and discursive analysis and powerfully arguing for technological measures for curbing the cybercriminal infrastructure that enables both attacks on critical infrastructure and influence operations. Recent examples, such as the Dutch financial-crime authorities' seizure of 800 servers in May 2026, have shown considerable promise in significantly disrupting the "backbone of some of Iran's most active cyber espionage campaigns."[7] This paper encourages policy makers and law enforcement agencies to move beyond such episodical targeting and adopt a methodical, sustained campaign that cripples the cybercriminal infrastructure underpinning these activities.

This paper is organized into three parts. Part 1 examines the blind spots in current counter-influence frameworks, reconceptualizing influence operations as a supply-and-demand market in which cybercriminal infrastructure plays a constitutive enabling role. Part 2 provides a technical taxonomy of that infrastructure across three categories: internet, financial, and operational.Part 3 sets out the strategic and policy implications of this framework and makes the case for a market-disruption approach to counter-influence. Recommendations follow the conclusions.

Part 1: Blind Spots in Current Counter-Influence Approaches

Key conceptual frameworks that targeted adversarial foreign influence operations emerged in the late 2010s and early 2020s. In 2020, the U.S. State Department's Global Engagement Center (GEC) found that "there is no single media platform where propaganda and disinformation are distributed."[8] This observation was accurate at the time it was published. Similarly, in 2018, Yochai Benkler published a pioneering study that described the spread of manipulated information as 'network propaganda.' Benkler found that the overall effect on beliefs and attitudes emerges from the interaction of a broad set of discrete sources — only some of which

[7] Check Point, "The Server Seizure That Affects Iran's Cyber Operations," Check Point, June 1, 2026.
[8] U.S. Department of State, Global Engagement Center, "Pillars of Russia's Disinformation and Propaganda Ecosystem," August 2020.

are controlled by the propagandist — that repeat various versions of a narrative across the information ecosystem.[9]

In response to these findings, countering influence operations in the late 2010s and early 2020s focused on detecting, exposing, and monitoring manipulated information (narratives), debunking and fact-checking these narratives, and offering pre-bunking information injections and media literacy training to reduce tractions of manipulated narratives.[10] These efforts were primarily reactive, seeking to counter malign narratives and networks of trolls and bots, while reducing manipulated content visibility and sanctioning actors who participated in manipulating and spreading false information.[11] In recent years, professionals in the field have been grappling with the limits of this approach and looking to move away from what can be seen to what can be disrupted.

Attention has increasingly shifted to the technological dimensions of influence operations, moving beyond narrative and network analysis. Since 2018, the U.S. government has employed disruptive tactics — including CYBERCOM and FBI action to cut internet access to Russian troll farms and seize domains supporting influence operations during the 2024 presidential election. These actions, however, were designed primarily as short-term responses to electoral threats rather than as components of a sustained framework.[12] By contrast, other countries have pioneered broader, long-term approaches. Taiwan has sought to counter Chinese "cognitive warfare" through rapid fact-checking and widespread public exposure within a whole-of-society resilience model.[13] Finland has embedded media literacy into its national education system from an early age, while Sweden established the Psychological Defence Agency in 2022 to counter 'psychological warfare.'[13] Yet despite these integrated efforts, all three states are experiencing a marked increase in the volume, sophistication, and aggression of foreign influence operations.[14]

In 2026, the EU recognised this ‘continued escalation’ and encouraged its partners to move ‘onto the front foot, marking a shift from a largely reactive to a proactive and anticipatory

---

[9] Yochai Benkler, Robert Faris, and Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (Oxford University Press, 2018).

[10] This includes the ABCDE counter-FIMI approach; see Debunk.org, “ABCDE Framework,” n.d.; U.S. Department of State, Learning Brief: Counter-Disinformation Literature Review, July 2023; DISARM Foundation, “DISARM Framework,” n.d.

[11] Raquel Miguel Serrano & Maria Giovanna Sessa, “Beyond Disinformation Countermeasures: Building a Response Impact Framework,” EU Disinfo LAB, November 29, 2024.

[12] Ellen Nakashima, “U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms,” *Washington Post*, February 26, 2019; U.S. Department of Justice, “Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere,” September 4, 2024.

[13] Swedish Psychological Defence Agency, “Our History,” n.d.

[14] Finnish Security and Intelligence Service (SUPO), “Joint Operation by Authorities Curbs Russian Cyber Espionage,” press release, April 8, 2026; Euractiv, “Sweden Says It Is Target of Russia-Backed Disinformation Over NATO, Koran Burnings,” n.d.

approach'.[15] The EU adapted the military concept of the 'kill chain' to map hostile influence operations across their distinct phases — from planning and financing to production and amplification.[16] It has called to disrupt 'the technical backbone of disinformation campaigns as a key direction for the development of counter foreign influence activities.[17]

The EU's kill chain framework represents an important step toward a more proactive approach. At the same time, it exposes a structural blind spot that undermines its effectiveness and points to a fundamental limitation shared by many liberal democratic responses to influence operations. It consistently fails to recognise the broader dynamic of supply, demand, and enabling infrastructure within which both state and non-state actors operate. Both US CYBERCOM's proactive measures and the EU's kill chain, for example, focus on the supply-side asset network — targeting actors circulating and amplifying manipulated information in a coordinated and inauthentic manner. In the EU's case, shortcoming stems from a terminological imprecision, with 'FIMI infrastructure' used as a loose relabelling of the threat actors' ecosystems already described by Benkler in 2018. Such thinking assumes that the actors sustaining the ecosystem that fuels many influence operations are identifiable, politically motivated, and vulnerable to reputational or legal costs. The cybercriminal infrastructure involved in influence operations fits none of those criteria. Instead, it operates through a Cybercrime-as-a-Service (CaaS) model and remains undetected to those who try to enforce countermeasures. The EU's own research illustrates this challenge, finding that 65 percent of detected FIMI activity could not be attributed.[18]

Cybercriminals operate as contractors who deliberately distance themselves from state sponsors, providing plausible deniability to clients while remaining largely invisible to the attribution processes that sanctions and law enforcement depend upon. Crucially, they are also fluid and replaceable: disrupting one node in a commercial supply chain — as CYBERCOM has done — does not break the chain if the underlying service can simply be repurchased from another vendor. This kill chain model, borrowed from a military logic of sequential and dependent phases, is poorly suited to a market-like structure where each link is fungible. A market-structured threat requires market-disruption logic, not a sequential list of actions.

Rethinking Influence Operations as a Supply, Demand, and Enabling Landscape

Incorporating cybercriminal infrastructure into the analytical framework reconceptualizes the dynamics in which influence operations function. It shifts the focus from state-directed activity to a market structure in which demand, supply, and enabling infrastructure operate as

---

[15] European External Action Service, "4th EEAS Annual Report on Foreign Information Manipulation and Interference Threats," March 12, 2026.
[16] European External Action Service, "4th EEAS Annual Report on Foreign Information Manipulation and Interference Threats," p. 20.
[17] Raquel Miguel Serrano & Maria Giovanna Sessa, "Beyond Disinformation Countermeasures: Building a Response Impact Framework," EU Disinfo LAB, November 29, 2024.
[18] European External Action Service, "4th EEAS Annual Report on Foreign Information Manipulation and Interference Threats," p. 9.

interdependent but semi-autonomous layers, connected by incentive and opportunity rather than command and control.

On the demand side, four distinct categories of actors, both foreign and domestic, create the conditions in which influence operations become viable and self-sustaining. The first category consists of foreign state principals — government ministries, security and intelligence agencies, spokespersons and others — who set strategic objectives and translate political goals into market incentives, commissioning the production of narratives and the deployment of asset networks available for influence operations. The second comprises domestic populist leaders who play a structurally distinct but equally important role: through a symbiotic relationship with foreign influence actors, they simultaneously benefit from content that legitimizes their political claims while domesticating foreign narratives by repackaging them through credible national voices. In doing so, they effectively "launder" the indicators of foreign interference that might otherwise alert audiences. The third category includes ideologically aligned domestic audiences. Shaped by pre-existing beliefs and information environments, these audiences create the receptive conditions that make influence operations viable. They give foreign state actors the confidence to invest and domestic populist leaders the incentive to participate in the spread of malign influence and adverse political interference. The fourth involves private sector platform operators — motivated by engagement-driven monetization rather than political intent — create structural demand conditions by building and maintaining the algorithmic environments in which manipulated content can scale at relatively low cost.

The supply and enabling side of the market is similarly layered. First, lower down the bureaucratic ladder, foreign state working-level actors produce the architecture of influence operations. These include in-house government departments and commercial contractors in foreign states who translate principals' political briefs into content ecosystems combining narratives, visuals, audio, deepfakes, and the distribution assets required to disseminate them — including bot networks, fake profiles, proxy outlets, and state-funded media organizations. The most notable examples include Russia's Social Design Agency and the Chinese PR firm Haixun, which have been contracted by the Kremlin and Chinese Ministry of Public Security (MPS), respectively, to deliver influence operations.[19]

Beneath this visible production layer sits a cybercriminal enabling infrastructure: internet infrastructure providers offering hosting, bulletproof servers, domain registration and VPN services; financial infrastructure, including payment processors, cryptocurrency channels, and ad-tech monetization systems; and operational infrastructure, including SIM farms, anti-detect browsers, and credential theft services that provide the anonymity and resilience operations require.

---

[19] Alberto Fittarelli, "PaperWall: Chinese Websites Posing as Local News Outlets with Pro-Beijing Content," The Citizen Lab, February 7, 2024; UK Government, "UK Sanctions Putin's Interference Actors," press release, October 28, 2024.

Crucially, this infrastructure is not purpose-built for influence operations — it exists and is self-sustaining through the far broader demand of financially motivated cybercriminals, for whom influence operations represent only a marginal share of overall activity. This has two implications for counter-measures. First, the infrastructure cannot be disrupted by targeting influence operations alone. Second, interventions directed at the infrastructure itself will consequentially degrade the scope and scale of influence activities.

Influence operations also benefit from an amplification layer and a feedback loop. Organic spread through unwitting amplifiers — journalists, influencers, and legitimate media outlets who repeat narratives without awareness of their origin — and algorithmically driven recommendation systems that refine audiences based on psychographic profiling and behavioral data, extend operational reach far beyond anything the commissioning foreign state directly controls. As Benkler rightly observed, the effects emerge not from a single story or source but from the fact that a wide range of outlets, most of which are not controlled by the propagandist, repeat various versions across the information environment.[20] This amplified content then returns to and reinforces ideologically aligned audiences, expanding demand over time and sustaining the market incentives that make further operations worthwhile. The circle closes not through coordination but through the structural alignment of incentives — which is precisely why interventions designed to break a sequential chain will need to adopt a market logic to target the foundational role of cybercriminals.

[20] Benkler, Faris, and Roberts, *Network Propaganda*.

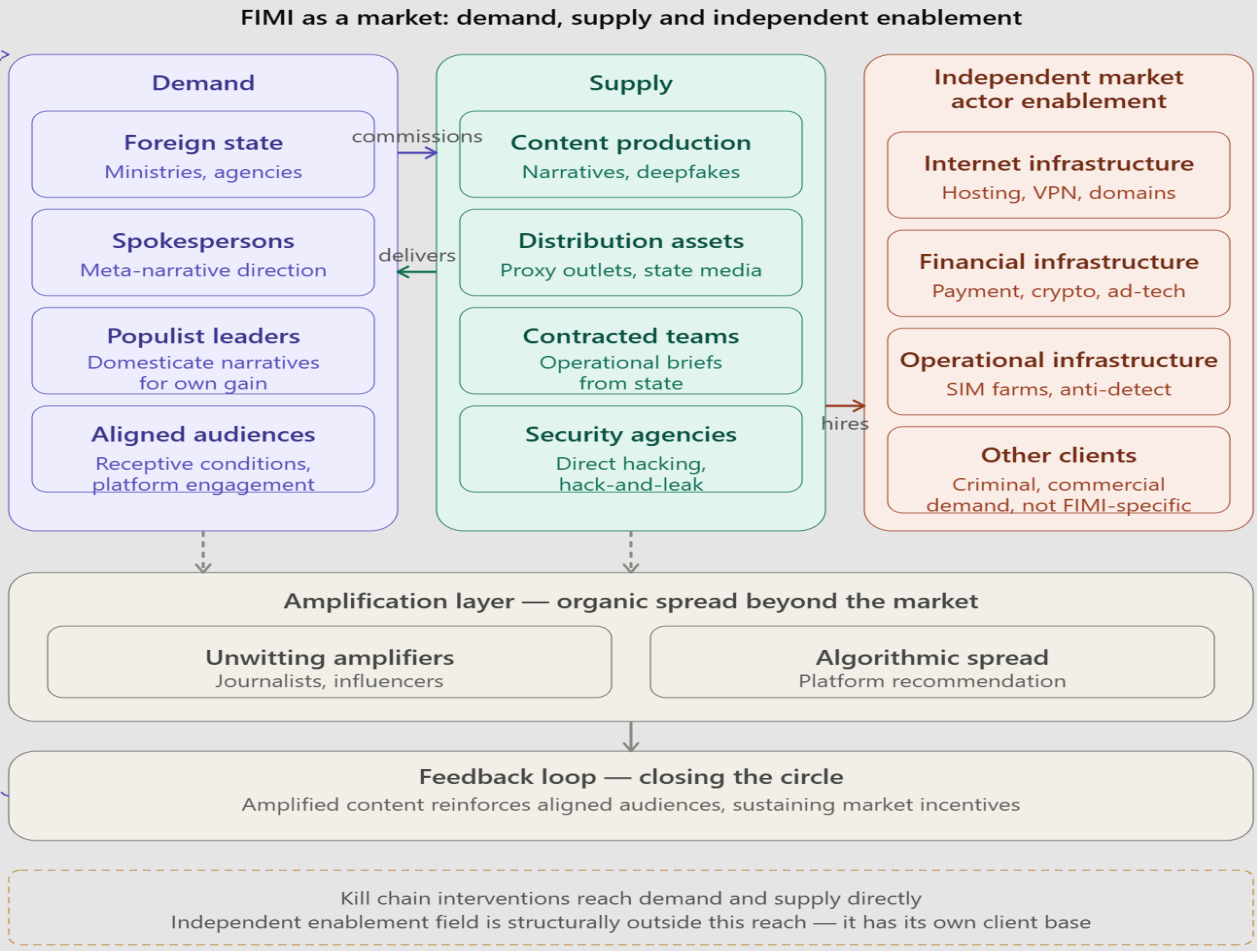


Figure: FIMI as a market structure with cybercriminal enablement as an independent actor field.

Why Now? Geopolitics, Tech, and the Rise of Cybercrime in Influence Operations

Amid heightened geopolitical competition and conflict, cybercriminal infrastructure has become both an enabler and a force multiplier for cyber-attacks and influence operations, offering authoritarian state threat actors cheap and effective means of targeting democracies through online operations. Google's February 2025 report, *Cybercrime: A Multifaceted National Security Threat,* traced this threat back to the earliest computer network intrusions, where financially motivated actors conducted operations for the benefit of hostile governments.[21] What was once a consistent but limited pattern of cooperation between state actors and cybercriminals is, however, hardening into a dangerous and symbiotic relationship — one in which influence operations represent an area of opportunity and growth.

Two interconnected, conflict-related dynamics drive this trend. Intensifying global conflicts have accelerated the use of online and cyber activity as a means of reaching distant targets without requiring a physical presence, while simultaneously creating pressure to reduce costs

[21] Google Threat Intelligence Group, "Cybercrime".

and identify more economical operational solutions. The Google report identified a marked intensification of cyber activity following Russia's full-scale invasion of Ukraine in 2022, which led the Kremlin to draw more aggressively on its latent pool of cybercriminals who could be paid or coerced into supporting state objectives.[22]

Russia has been a leader in blurring lines between state-sponsored and criminal activities. In March 2022, when Vladimir Putin's plans for a quick operation in Ukraine were thwarted, the Kremlin turned to Wagner PLC, a Kremlin-backed mercenary group, to fill gaps on the front line through a scheme of expropriations of convicted felons. Since then, criminality has been ever more explicit in state-sponsored activities, with cybercriminals becoming an integral, and even celebrated, part of state efforts, in full public view.

As part of this 'criminal turn' in Russian state activities, Russia's security and intelligence services have developed a symbiotic relationship with pro-Russian hacktivist groups, using them as a plausibly deniable instrument of cyber-enabled influence operations and attacks on critical infrastructure. For instance, in 2026, Sweden accused a pro-Russian group with links to Russia's security and intelligence services of conducting a cyberattack on a heating plant — an announcement that followed similar warnings issued by officials in Poland, Norway, Denmark, and Latvia.[23]

While Russian security agencies have traditionally maintained an arm's length relationship with cybercriminals and hacktivist groups, the boundaries of that arrangement are shifting — with formal acknowledgement of these actors as constituent parts of Russia's war effort becoming increasingly visible. A US-Russia prisoner swap in August 2024 was a good illustration of this process.[24] Media attention focused on high-profile Russian operatives who were accused of sabotage and espionage in the West, such as Vadim Krasikov, who was serving a life sentence for carrying out an assassination in a Berlin park, and a family of deep-cover Russian agents in which the parents, Anna and Artyom Dultsev, who were a real-life version of the TV series *The Americans*.[25] Interestingly, the list of Russian released prisoners included two Russian cybercriminals: Roman Seleznev and Vladislav Klyushin. Seleznev was sentenced in the United States in 2017 to 27 years in prison for computer hacking crimes[26], and Klyushin, who ran a Moscow-based information technology company, was convicted of wire fraud and securities fraud in the United States in 2023.[27] Upon their return to Russia, both men were personally

---

[22] Google Threat Intelligence Group, "Cybercrime".
[23] Claudia Ciobanu and Emma Burrows, "Sweden Blames Pro-Russian Group for Cyberattack Last Year on Heating Plant," Associated Press, April 15, 2026. For other examples of pro-Russian hacktivists working with Russian intelligence agencies, see Google Threat Intelligence Group, "APT44: Unearthing Sandworm," Google Cloud Blog, April 17, 2024; Recorded Future, "Anatomy of DDoSia," July 22, 2025.
[24] BBC News, "Russia–U.S. Prisoner Swap," BBC, August 2, 2024.
[25] Ibid.
[26] U.S. Department of Justice, "Russian Cyber Criminal Sentenced to 27 Years in Prison for Hacking and Credit Card Fraud Scheme," press release, April 21, 2017.
[27] Associated Press, "Russian Man with Kremlin Ties Gets 9 Years in US Prison for Hacking and Insider Trading Scheme," September 7, 2023.

welcomed home by President Putin in a reception typically reserved for individuals who have committed exceptional service to the state. These unusual scenes represent a growing recognition by the Russian authorities of the importance of the services rendered by cybercriminals to state efforts.[28]

In Russia's case, this addressed a practical challenge facing the Kremlin. Western governments' decisions to expel large numbers of Russian diplomats and drastically reduce Russian diplomatic presence significantly diminished Russia's physical asset base in target countries,[29] creating a capability gap for conducting operations on the ground. Cyber and influence activities and reliance on both cybercriminals and offline criminals are increasingly filling this gap. However, this pattern is by no means unique to Russia.

China has constructed a formal market for contracted cyber and influence operations, in which private information security companies and PR firms compete for government contracts to conduct hacking and content distribution on behalf of the Ministry of State Security and the Ministry of Public Security.[30] The 2024 leak of documents from i-Soon — a Chinese cybersecurity contractor — revealed a company responsible for compromising at least fourteen governments, pro-democracy organizations in Hong Kong, universities, and NATO.[31] In March 2025, the US Department of Justice indicted twelve Chinese nationals connected to i-Soon, finding that these actors conducted intrusions both at the direction of the state and on their own initiative, brokering stolen data to government clients while also selling it to third parties for private profit.[32] Chinese state agencies have granted contractors tacit permission to conduct financially motivated side activities, tolerating criminal behavior as the implicit price of maintaining a flexible, deniable capability outside the formal People's Liberation Army (PLA) hierarchy.[33]

Another example is the ecosystem Google tracks as GLASSBRIDGE: Chinese public-relations and marketing firms, including Shanghai Haixun Technology and Shenzhen Haimai Yunxiang Media, disseminate pro-PRC content at scale through inauthentic news websites. Google states that it cannot attribute who hired these firms, though it assesses that the companies may take

---

[28] Lukasz Olejnik, "Russian Cyber and Information Warfare and Its Impact on the EU and UK," KCL Policy Institute, April 15, 2025.
[29] Kate Connolly, "EU Allies Expel Over 120 Russian Diplomats in Two Days After Bucha Killings," *The Guardian*, April 5, 2022.
[30] AJ Vicens, "Chinese Hackers Are Increasingly Deploying Ransomware, Researchers Say," CyberScoop, June 26, 2024.
[31] Dakota Cary and Aleksandar Milenkoski, "Unmasking I-Soon: The Leak That Revealed China's Cyber Operations," SentinelLabs, February 21, 2024.
[32] U.S. Department of Justice, "Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Hacking Operation," press release, March 5, 2025; Federal Bureau of Investigation, "Beijing Leveraging Freelance Hackers and Information Security Companies to Compromise Computer Networks Worldwide," alert, March 5, 2025.
[33] Antonia Hamaidi, "Here to Stay: Chinese State-Affiliated Hacking and Strategic Goals," MERICS, November 22, 2023.

direction from a shared customer.[34] The activity has reached audiences in Brazil, India, Kenya, South Korea, and beyond.[35] Together, i-Soon and GLASSBRIDGE illustrate how contractors and commercial services expand the Chinese influence ecosystem beyond direct vertical command and control.

Iran presents a structurally different but equally instructive model. Its intelligence agencies, led by the Iranian Revolutionary Guard Corps (IRGC) and Ministry of Intelligence and Security (MOIS), conduct their own operations alongside a patchwork of front companies and other entities.[36] Tehran has increasingly outsourced network access to the cybercrime underground, posting hacked databases on criminal forums to incentivize them to target Israelis providing ransomware affiliates with discounts for targeting Israeli entities, and more. In doing so, it has effectively converted state espionage infrastructure into a revenue-generating criminal service.[37] A joint advisory from the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Defense Cyber Crime Center in August 2024 identified Iranian state-linked actors exploiting vulnerabilities to gain initial access to victim networks before handing compromised systems to ransomware affiliates such as NoEscape, RansomHouse, and ALPHV/BlackCat, in exchange for a share of the ransom payments.[38]

By 2026, the boundary between state-sponsored activity and organized cybercrime has not merely blurred — it has, for operational purposes, transformed into a symbiotic relationship. This process is a culmination of decades of forming and cultivating these relationships, which are coming to the forefront of public attention driven by intensifying global conflict and advances in AI which are reducing the costs of entry into the cybercrime world.

Often referred to as Cybercrime-as-a-Service (CaaS) this phenomenon forms one part of a broader holistic threat that state threat actors' use of criminals poses to liberal-democracies, enabling cyber-attacks, influence operations, and works in unison with other forms of cyber-enabled hybrid threats, such as ‘Violence-as-a-Service’.[39] Yet Western governments and cybersecurity firms distinguish between politically motivated, state-backed cyber and influence operations and financially motivated cybercriminal activities. This distinction is a dangerous oversight that limits the ability to counter these threats. The next part of this paper will demonstrate the key role of cybercriminal infrastructure in enabling influence operations.

---

[34] Google Threat Intelligence Group, “Seeing Through a GLASSBRIDGE: Understanding the Digital Marketing Ecosystem Spreading Pro-PRC Influence Operations,” Google Cloud Blog, November 22, 2024.
[35] Ibid.
[36] Insikt Group, “Leaks and Revelations: IRGC Networks and Cyber Companies,” Recorded Future, January 25, 2024.
[37] Halcyon Research, “Pay2Key: Iranian-Linked Ransomware Is Back Again,” n.d.
[38] America's Cyber Defense Agency, "Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations," 2024, August 28.
[39] Thomas Brewster, “The Wiretap: The Worrying Rise of Violence-as-a-Service,” Forbes, April 29, 2025.

Part 2: The Unholy Trinity: Cybercrime, Cyber Operations, and Influence Operations

Anyone who has read a threat intelligence report on influence operations in the past year is likely familiar with the large number of accounts being taken down. For example, Google TAG publishes a quarterly report detailing the disruption of thousands to tens of thousands of YouTube channels and other Google entities, and Meta publishes similar numbers in its own periodic threat reporting. These figures are often taken at face value by the threat intelligence community, creating the impression that state actors can effortlessly generate and sustain tens of thousands of online accounts or entities. Yet is it, in fact, that easy? In practice, it is considerably more complex. This section will delineate and describe the underlying cybercrime infrastructure that enables nation-states to carry out influence operations at scale. While much of this infrastructure overlaps with traditional cybercrime infrastructure used for cyber operations, much of it exploits previously unexplored fields of infrastructure, such as black-hat marketing capabilities.

Cybercriminal Infrastructure

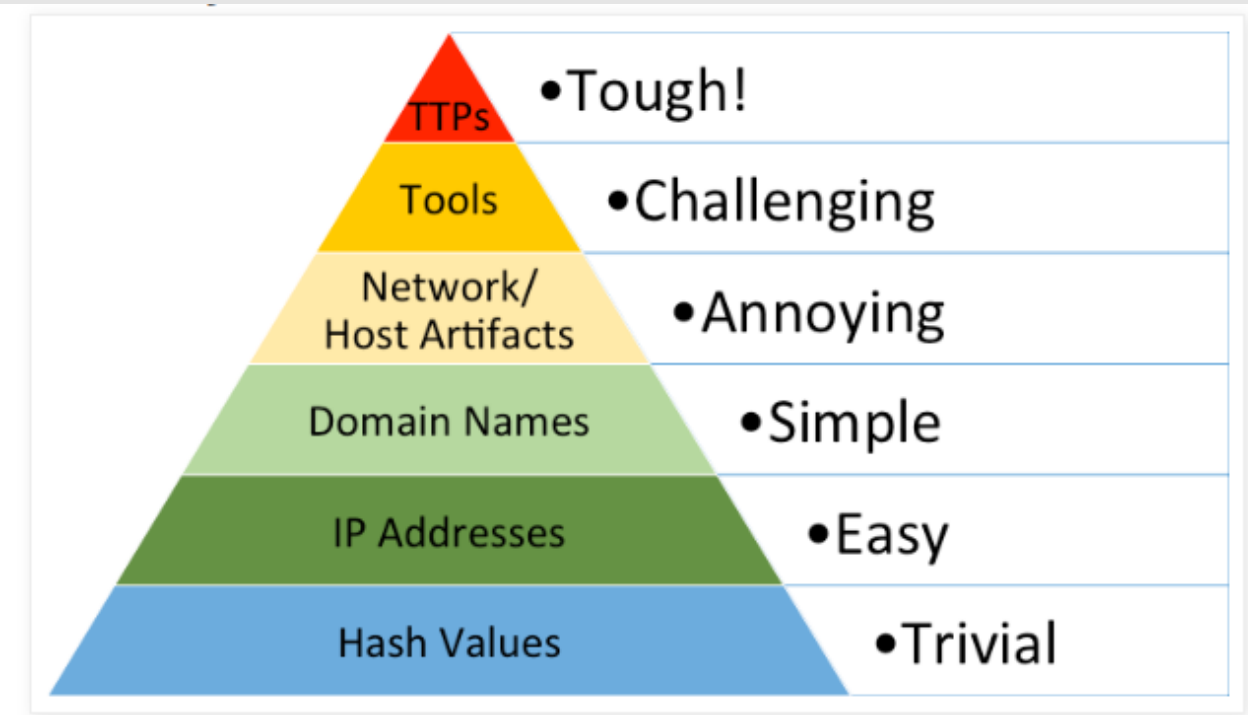
In the context of this paper, the term "infrastructure" refers to the foundational tools, functions, and services needed to run operations online in a broad sense. These include, but are not limited to, payment capabilities, browsing software, servers, and capabilities such as purchasing accounts and online entities, engagement, and other services. These correspond broadly to the three enabling-infrastructure categories examined below: internet, financial, and operational.

First, focusing on the content, narratives, and networks (at best) of social media accounts misses the broader forest for the trees. Such research, while useful, looks only at the final stage of the operation. Influence operations, like operations of any kind, do not materialize out of thin air, but rather are crafted — carefully or not — by actors in multiple stages. The process of running an operation, similar to cyber operations, is called a "kill chain."[40] Shifting the emphasis on research from the end-product of the operation to the tooling and infrastructure used by threat actors enables counter-influence operations teams to move up the kill chain, adding increasingly significant friction to threat actors.

A useful analogy from the cyber world is the "Pyramid of Pain," conceptualized by David Bianco. Focusing on indicators relevant to cyber operations — from easily-replaced and disposable infrastructure such as domain names, IP addresses, or file hashes to less-easily replaced capabilities such as tooling and tactics, techniques, and procedures (TTPs) — the pyramid "shows the relationship between the types of indicators you might use to detect an adversary's activities and how much pain it will cause them when you are able to deny them those indicators." Applied to influence operations, the same logic holds: disruption is most effective

[40] Microsoft, "What Is the Cyber Kill Chain?" n.d.

not at the level of accounts and content — the cheapest layer to replace — but in the foundational infrastructure that cannot be quickly repurchased.[41]



Source: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

This concept, well-known in cybersecurity, has yet to be applied to influence operations, despite the framework being almost entirely analogous. Moving beyond the disposable — accounts instead of hashes, domains and IP addresses remaining relevant to both — and focusing instead on foundational tooling and capabilities would enable threat intelligence analysis focusing on influence operations to move up the pyramid and impose disproportionate and lasting friction on adversarial operations.

Second, focusing on infrastructure is often more conducive to garnering political support. Infrastructure is relatively apolitical and does not require researchers analyzing influence operations to verify information and make value judgment calls about its veracity.

Third, focusing on infrastructure, tooling, and technical capabilities is a requisite demand for countering contemporary hybrid threats. While many Western countries continue to view influence operations as a siloed form of activity, adversarial countries do not, fusing them into all of their activities— whether covert or overt. Russia and Iran, for example, consistently run cyber-enabled and physical influence operations, whereas Chinese operators have begun

[41] David Bianco, "The Pyramid of Pain," Enterprise Detection & Response, March 1, 2013.

conducting long-term, strategic communications campaigns supported by covert influence operations.[42]

Fourth, cyber operators are already making increasing use of criminal infrastructure. Russian and Iranian actors such as Void Blizzard and Aria Sepehr Ayandehsazan, among others, have already been known to use criminal hosting services for domain registration, residential proxies, and data sourced from criminal markets.

Lastly, focusing on infrastructure exploits the moment threat actors are most exposed: not during the planning stage, when activity is largely private, but during dissemination, when tooling and accounts become observable to platforms and governments alike. Threat actors can easily prepare operations without exposing their activity prior to running them, only once they launch them, they truly become vulnerable to disruption. This dynamic has been exacerbated with generative AI, which has already been shown to accelerate the creation of content and even set up infrastructure, all with the potential of being run locally.[43] What generative AI cannot easily resolve is the key bottleneck of influence operations: dissemination across online platforms. Law enforcement and intelligence agencies actively monitor online platforms and the broader internet for misuse — be it hostile foreign influence, fraud, or other malicious activity — making it difficult for threat actors to exploit them at scale. Effective dissemination, however, requires broad access as well as the ability to post content at scale. Doing so requires a wide range of infrastructure, such as hosting services, residential proxies, accounts, and more. These are most readily and cost-effectively available through criminal services, ranging from the infrastructure needed to connect to and use the internet, financial infrastructure, and operational infrastructure for social media platforms and other uses.

Internet Infrastructure

The first category of criminal infrastructure is the foundational infrastructure used by threat actors to connect to and operate on the internet. This includes the use of proxy services, virtual private servers (VPS) and RDP (remote desktop protocol) instances, VPN providers, anti-detect browsers, and other foundational infrastructure. These services are the most foundational of capabilities, enabling threat actors to browse the internet while avoiding detection by platforms and hostile governments.

Proxy services are one of the most commonly used and critical capabilities. Proxy services, be they residential or mobile, are what enable threat actors to browse the internet. For operational security or practical reasons, threat actors are unable or unwilling to rely on commercial VPN services and instead turn to proxy services to access the internet without exposing their public IP address. This capability is critical to every stage of an influence operation. From collecting data and researching targets to connecting to legitimate services and platforms and beyond,

---

[42] Ari Ben Am, "A Year of Meming Dangerously: Iran's Influence Operations Targeting Israel Since October 7," Foundation for Defense of Democracies, August 28, 2025.
[43] Insikt Group, "Adversarial Intelligence: Red-Teaming Malicious Use Cases of AI," Recorded Future, March 19, 2024.

threat actors must have access to proxy services to avoid detection. Criminal services are the most common, though legitimate residential and mobile proxy services do exist.

Residential proxies are the most widely used type of proxy. Criminal residential proxies allow their end users to route their traffic via unwitting residential networks and users. As a result, their traffic appears to online platforms and services as though it originates from a legitimate residential network, making them more trusted. This is especially needed to appear legitimate online, as most VPNs and TOR exit nodes are all mapped and known to providers, which either block those connecting from suspicious exit points or require additional verification. Residential proxies are useful for routine browsing, connecting to accounts, and automating other types of activity, such as data collection.

Mobile proxies are also useful. Similar to residential proxies, threat actors can rent access to networks of mobile devices operating on cellular networks, mainly 4G and 5G. Because the traffic originates from legitimate mobile devices using cellular data, it appears less suspicious to online platforms and is considerably harder to block at scale. As with residential proxies, criminal mobile proxies exist to enable end users to automate activity on online platforms, scrape data, or otherwise access the internet.

These services are used frequently in cyber espionage. Criminal proxy services have been identified as supporting nation-state and advanced persistent threat (APT) cyber operations.For example, Spur analyzed a campaign that the source of a leak attributed to Kimsuky — an attribution Spur explicitly said it did not validate — and found use of the Chinese WgetCloud proxy service.[44]

While residential proxy services often utilize compromised routers and edge devices to route their traffic, in some cases individuals willingly sell access to their home networks. Research on the Belarusian proxy company DSLRoot found that it provides access to US-based residential proxies, including those hosted by US servicemembers, in exchange for a fee paid to those who provide access to their home networks.[45]

While primarily used for cyber operations or cybercrime, residential and mobile proxies have been exploited in the past for influence operations or influence operation-adjacent activity. For example, leaked documents originating from the Iranian threat actor APT 35 indicate that one of the group's operators was responsible for acquiring and connecting proxies to accounts purchased online. Although these accounts were presumably used for phishing operations, the exact same modus operandi could be employed to run purchased or hacked accounts.[46]

Proxies are a foundational tool used for all types of illicit online activity and are therefore a key focus of law enforcement efforts. Google's Threat Intelligence Group, alongside multiple law

---

[44] Spur, "How Spur Uncovered a Chinese Proxy and VPN Service Used in an APT Campaign," August 20, 2025.
[45] Infrawatch, "Belarus-Linked DSLRoot Proxy Network Deploys Hardware in U.S. Residences, Including Military Homes," February 7, 2026.
[46] Ari Ben Am, "The Inner Machinations of a Threat Actor," Memetic Warfare (newsletter), October 3, 2025.

enforcement agencies and other partners, took down IPIDEA, the world's largest illicit residential proxy provider.[47] According to Google, this operation took down millions of available proxy devices, which they estimate as having a significant downstream effect on threat actor capabilities.

Proxies are critical to operations of all kinds, but are not sufficient on their own. Threat actors also need access to environments in which they can run relevant software, be it for command-and-control (C2) infrastructure supporting cyber or influence operations, hosting domains, or other operational purposes. Unable or unwilling to invest the effort needed to break the Know-Your-Customer (KYC) procedures of legitimate vendors, or to expose their operations to infrastructure hosted in foreign countries, threat actors often elect to rent infrastructure from illicit bulletproof hosting services.[48] In some cases, however, bulletproof hosting firms are able to exploit legal loopholes or lax regulatory environments to provision infrastructure legally to threat actors, as illustrated by the recent Iranian utilization of European hosting firms that explicitly define themselves as bulletproof hosting providers.[49]

The environments needed are usually either virtual private servers (VPS) or Remote Desktop Protocol (RDP) instances. These services are virtualized instances of a given operating system, be it Windows Server, Linux distributions, or others. Threat actors can rent these services from bulletproof hosting providers for relatively modest monthly fees, often only a few dozen US dollars. VPSes and RDP instances can then be used to deploy software and capabilities globally with minimal friction and visibility, most commonly for hosting domains used in cyber and influence operations, such as hacked data laundered on leak sites. Other types of servers, such as SMTP servers for distributing large volumes of email, can also be rented from many of these providers.

While bulletproof providers are of significant use to threat actors for influence operations, they are often insufficient on their own. Most bulletproof providers and their IP ranges are known and actively tracked by governments, platforms, and information security companies. Their utility may therefore be limited, as entire Autonomous Systems (AS) or IP ranges can be blocked en masse.

This issue can be remedied by using host providers in legitimate ranges, often based in Western countries. Accessing such services, however, requires illicit financial infrastructure.

Financial Infrastructure

Financial infrastructure is also critical to enabling all types of influence operations. Criminal financial infrastructure is one of the largest categories of illegal services available online, catering to threat actors of varying scales. These services exist to fill several needs, mainly the

---

[47] Google Threat Intelligence Group, "No Place Like Home Network: Disrupting the World's Largest Residential Proxy Network," Google Cloud Blog, January 29, 2026.
[48] Bulletproof hosting services are illicit providers of hosting, server infrastructure, and related capabilities. These services do not comply with foreign law enforcement requests and often accept payment via cryptocurrency.
[49] Ari Ben Am, "Hacking with the Starlinks," Memetic Warfare (newsletter), January 22, 2026.

ability to pay anonymously for services online, to receive payment for services online or from online platforms (such as ad platforms), to launder funds, and to create anonymous financial infrastructure.

These services include multiple categories and capabilities. A popular service for threat actors is a virtual credit card service, in which an actor pays a third party to use a credit card unaffiliated with the paying party. This is important to be able to purchase goods and services online, such as hosting services or otherwise, from legitimate providers. Other services include "cashout" services, enabling threat actors to receive payment generated through scams or other illicit online activity into their accounts. Cryptocurrency mixers are another widely used service, allowing actors to run their cryptocurrency via a set of randomized wallets to obscure the origin of their funds.

At a small scale, threat actors often use commercially available online services of all kinds. From AI tooling and hosting services to productivity software, payment providers, advertisement services and beyond, threat actors often seek — and succeed — in acquiring access to legitimate services. Some services, such as hosting providers and payment processors, impose increasingly stringent Know Your Customer (KYC) requirements as the scale of use increases. Threat actors seeking to access these legitimate services must therefore be able to provide some form of basic identification and, in some cases, satisfy additional verification requirements. Threat actors can bypass KYC measures via a number of methods. These include purchasing hacked or otherwise illegally acquired ID cards, using generative AI to generate inauthentic IDs, relying on available criminal template services to produce fake bills and other forms of identification and documentation. Many of these capabilities are available primarily through the black-hat marketing subsection of the cybercriminal online underground and are rapidly growing in sophistication and use. Microsoft's 2025 Digital Defense Report found that the use of AI-generated IDs increased by 195 percent from 2024-2025.[50]

Circumventing KYC requirements, however, is just the first step. Payment must also be rendered to legitimate services, and a range of criminal services exist for this purpose. For smaller-scale operations, virtual credit card services may suffice. These services offer the use of a third party's credit card in exchange for a substantial commission on the amount charged.[51] Other options, such as virtual, single-use credit cards that are commonly used for legitimate purposes, can also be used for payment for criminal purposes.[52] The Belarusian proxy service DSLRoot, for example, also offers multiple virtual credit card services, including those that accept cryptocurrency to charge the cards, further enabling the bypassing of traditional financial services.[53]

---

[50] Microsoft, "Microsoft Digital Defense Report 2025," 2025.
[51] BlackHatWorld, "Virtual Credit Card Service?" BlackHatWorld Forums, archived April 5, 2025.
[52] Microsoft, "Microsoft Digital Defense Report 2025," p. 34.
[53] Infrawatch, "Belarus-Linked DSLRoot Proxy Network Deploys Hardware in U.S."

While legitimate providers may be exploited for small-scale operations, doing so carries a significant risk of exposure and takedown and is generally not viable for large-scale or long-term operations. This is due to the inherent nature of illicit financial tooling, which is often unavailable or effectively blocked at scale by legitimate providers. Legitimate vendors also often monitor their services for misuse, ensuring that any potentially risky customers are banned if identified as abusing payment methods or their platforms.

The difficulty of exploiting legitimate platforms at scale necessitates the use of illicit services by any nation-state threat actor. Cryptocurrency is a key enabler of these illegal or crypto-friendly services. While legitimate cryptocurrency payment processors and companies often impose stringent KYC requirements, many do not, particularly those based outside of the United States and Europe. Others don't require KYC at all. Regardless of whether KYC procedures are required, the public nature of all cryptocurrency transactions poses a risk of exposure for many, creating a demand for cryptocurrency mixers that can obscure the movement and origin of funds. While effective at small or even medium scale, large-scale exploitation of legitimate services and platforms requires substantial financial infrastructure, which is often achieved by setting up a front company. Threat actors have invested in setting up front companies for multiple purposes, ranging from operating as a front domestically and evading detection by foreign intelligence services to masking their activities abroad. While useful domestically for obfuscation, the main operational function of the front company is to facilitate the acquisition and establishment of infrastructure.

Front companies can be used to acquire and set up infrastructure in two ways. The first is to set up a front company in the state in which the actor is based, or in a friendly, nearby state, and to use that company to rent online infrastructure in its name. This method enables the company's use of conventional payment methods, such as credit cards or bank transfers, although it carries the risk that the front company itself may be exposed. This is especially effective if purchasing services from grey- or black-market providers.

The second method, in which the actor opens a company or financial entity in the country or region in which the actor seeks to operate or target, is a high-investment move but one that reaps higher dividends. Registering a company in the target area provides the actor with one paramount advantage: the ability to easily acquire high-value infrastructure in the area targeted.

Acquiring such infrastructure in the target area itself confers multiple advantages, namely the ability to more easily create accounts on local platforms without relying on VPNs or routing traffic via other methods to reduce the risk of detection by either the platforms themselves or domestic law enforcement agencies. Outward-looking intelligence agencies, for example, are often unable to investigate domestic activity. Combined with domestic privacy laws which can be exploited to mask ownership, the chance of being identified is that much lower.

Lastly, establishing a company in the target region enables a threat actor to acquire infrastructure at a much larger scale. For example, a threat actor could open a hosting company or other service provider that has an outwardly legitimate use case for creating and managing

significant infrastructure, such as Autonomous Systems (AS), meaning IP ranges, to a large number of servers or otherwise.

An additional advantage of setting up a front company in a target area of operations is the exploitation of that country's justice system. Most democratic countries impose strict limits on which organization or agency can investigate what activity within their own borders. For example, in the United States, setting up a front company domestically prevents much of the US intelligence community from monitoring or investigating malign activity, thereby significantly reducing the risk that domestically conducted operations will be detected. Threat actors, be they nation-state or financially motivated cybercriminals, have exploited lax corporate registration requirements in Western countries for years. Threat actors also often utilize the same resources and tooling they use to create inauthentic accounts and purchase infrastructure for the purpose of company registration, such as forging documents or using breached personal data. Certain countries have been especially lax, such as the United Kingdom. In one extreme case, over 11,000 Chinese companies fraudulently used the address of a single British citizen to register their businesses, leaving him with an exceptionally large tax bill.[54]

Iran and Russia have also exploited European countries for similar end goals. Leading Iranian cyber and influence operations threat actor Aria Sepehr Ayandehsazan (ASA) set up two front companies, Server-Speed and VPS-Agent, exploiting the Lithuanian hosting reseller BACloud to provision infrastructure for its own operations.[55] ASA also used these companies to provide technical and hosting support to individuals operating from Lebanon and to Hamas-affiliated or Hamas-themed websites.

Russian influence threat actors such as the Social Design Agency (SDA), responsible for the prominent Russian influence operation "Doppelganger," contracts a web of Russian bulletproof hosting providers, including the recently-sanctioned Aeza, for hosting domains and other infrastructure.[56] These bulletproof hosting providers themselves have set up front companies in the EU, Singapore, and elsewhere to mask their own activity and gain access to legitimate hosting infrastructure.[57] Doppelganger has also utilized the bulletproof hosting provider Stark industries, which has been exposed as creating European front companies, to host infrastructure in Europe.[58]

Threat actors have of course also utilized front companies in the United States for cyber operations. Threat actors have been exposed as using US-registered LLCs, particularly in

---

[54] BBC News, "Cardiff Flat Owner Gets Tax Bills for 11,000 Chinese Firms," April 7, 2023.
[55] Federal Bureau of Investigation, U.S. Department of the Treasury, and Israel National Cyber Directorate, "New Tradecraft of Iranian Cyber Group Aria Sepehr Ayandehsazan aka Emennet Pasargad," October 30, 2024.
[56] U.S. Department of the Treasury, "Treasury Sanctions Global Bulletproof Hosting Service Enabling Cybercriminals and Technology Theft," press release, July 1, 2025.
[57] Qurium, "How Russia uses EU companies for propaganda: Exposing the Evil Empire of Doppelganger Disinformation," July 11, 2024.
[58] Ibid.

Wyoming, as front companies to rent servers and infrastructure in the United States for cyber operations.[59] This same model can also be applied to influence operations.

While legitimate financial infrastructure is key to acquiring necessary services and tooling, many of the capabilities used by threat actors are themselves available through the cybercrime underground. This ecosystem operates not only on the "dark web," but also primarily on the clear web and messaging applications such as Telegram, serving as a catalyst for threat actor activity. These tools are used primarily for criminal purposes, including spam, scams, phishing, and even higher-impact crime such as ransomware. They exist independently of their use for influence operations, as their operators and proprietors are profit-motivated.

Without the existence of these tools, adversarial nation-states would have to invest significant resources in developing and maintaining such capabilities. While many nation-state actors could certainly surmount this and develop these capabilities in-house, their existence on the market enables threat actors of all levels to operate at scale and at considerably lower cost. Most of the infrastructure needs of threat actors are foundational, meaning that they serve as key capabilities that enable basic functioning and operations. However, many operational capabilities used by threat actors are commercially available via unscrupulous vendors in certain countries or by criminal vendors online. These comprise the bulk of the final category of infrastructure examined in this paper: operational infrastructure.

Operational Infrastructure

Operational infrastructure encompasses the tooling and services that enable key operational functions beyond internet access. Many of these are available from legitimate vendors for legitimate purposes or are used for cybercrime purposes unrelated to nation-state operations. A key example is SMS spam. Sending SMS messages on a massive scale is a key vector for influence and psychological operations, enabling threat actors to target large audiences based on location or phone number, which can be easily acquired via data breaches or other online sources. SMS messages can be sent at scale through two main capacities.

The first is the SIM farm, which can be set up by an actor or rented from spam farms. SIM farms coordinate dozens, hundreds, or even thousands of individual devices, as well as virtual, emulated devices and eSims, to send SMS messages (or messages through platforms such as WhatsApp, Telegram, or Signal) at scale to target numbers.[60] SMS farms are used primarily for scams, with large scale operations often using tens of thousands of SIM cards managed through multiple servers and dedicated hardware.[61]

This method has been used by Russia, as well as by actors suspected of being Iranian, as part of wartime operations. One Russian example used a mass-SMS and messaging capability to target

[59] Raphael Satter, "How Cybercriminals Are Using Wyoming Shell Companies for Global Hacks," Reuters, December 12, 2023.
[60] Itamar Eichner, "National Cyber Directorate Warns of SMS Attempting to Solicit Cooperation with Iran," Ynet, December 18, 2025.
[61] Europol, "Cybercrime-as-a-Service Takedown: 7 Arrested," press release, October 17, 2025.

Ukrainians with messages bearing a radio frequency that Ukrainians could use to surrender to Russian forces.[62] During the recent war, Israelis received inauthentic SMS messages impersonating the IDF Home Front Command and instructing them to avoid shelters in case of missile strikes.[63] In additional incidents suspected of being Iranian, mass SMS messages sent to Israelis included recipients' personal information to heighten their psychological impact.[64]

SMS messages can also be used to target populations within a specific geographic area. SMS blaster devices, which can be purchased commercially in many countries, enable the threat actor to impersonate a local cell tower, forcing all incoming and outgoing mobile traffic to be routed via their device. Although primarily used for scams,[65] there have also been reported cases of SMS blasters being used to disseminate malicious links to targets for non-financial reasons.[66] SMS blasting could have potent capabilities in contacting populations in urban centers with targeted messaging via covert operators active in a specific area.

Phone calls may also be used to reach broad populations as part of influence operations. Iranian actors, for example, have used commercially available automated calling services to contact Israelis on a large scale.[67]

Illicit services are also a key method for contacting targets. Black-hat marketing services offer many of the above legitimate services but without KYC processes or other limitations that prevent threat actors from abusing legitimate providers for influence and cyber operations. Illicit service providers also offer other solutions, such as direct messaging on online platforms. Mass direct messaging (DMing) is an inherently illegal or otherwise illicit service, as it requires the existence of a significant number of accounts on the target platform to distribute direct messages to a target audience.

Creating or acquiring massive amounts of online accounts is a key capability of the cybercrime underground that enables influence operations beyond mass DMing. Illicit service providers can provide accounts of all kinds to those interested in purchasing them, obtained through methods including exploiting breached data to take over accounts, registering accounts themselves, or otherwise. Such accounts can then be sold directly to the end client, providing them with a substantial online presence.

---

[62] Ari Ben Am, "Memetic Warfare Weekly: What's the Frequency?" Memetic Warfare (newsletter), October 2, 2023.
[63] Korin Elbaz-Alush, "Cyberattack Sends Israelis Rushing for Cover with Fake Emergency Texts," Ynet, September 19, 2024.
[64] Charlie Summers, "Thousands of Israelis Get Texts with Their Personal ID Number in Suspected Iranian Operation," *Times of Israel*, January 4, 2026.
[65] Daryna Antoniuk, "Greek Police Arrest Scammers Using Fake Cell Tower Hidden in a Trunk," The Record, January 21, 2026.
[66] National Cyber Security Centre (Switzerland), "Week 36: New risk from 'SMS blasters'," September 9, 2025; NetAskari, "SMS Blaster in the Wild," Substack, n.d.
[67] Dana Karni and Catherine Nicholls, "Hundreds of Israelis Receive Recruitment Calls from Iranian Intelligence, Police Say," CNN, September 27, 2025.

These accounts are managed by another subsection of the criminal online ecosystem: anti-detect browsers. Anti-detect browsers are most commonly used by cybercriminals for spamming, scamming, and other illicit online activities, and are developed and licensed out by other cybercriminals who develop them. These browsers provide APIs and automation capabilities that enable threat actors to set up multiple sessions, each associated with an individual account and proxy, while configuring technical indicators such as its user agent to enable account registration and activity online.

Accounts can also be used to sell engagement to amplify content online or impact platform algorithms. NATO's Strategic Communications Centre of Excellence researched this ecosystem on a number of occasions, finding that all leading social media platforms are vulnerable to varying degrees of inauthentic engagement, such as likes, comments, and shares, despite the use of automated detection systems and threat intelligence teams.[68] Threat actors frequently use these services to rapidly amplify their content. A recent Reuters investigation, for example, identified signs of inauthentic engagement in an influence operation conducted by a Philippines-based company on behalf of the Chinese embassy. The operation's entities, such as its TikTok account, exhibited signs of automated comments and YouTube videos with hundreds of likes but no comments or other forms of engagement.[69]

Illicit services are also available for running advertisements. Ad cloaking, a practice in which ads that would otherwise violate platform policies—primarily for financial, but also potentially for malvertising or political advertising— is routinely offered. This practice often presents one ad and URL to the verifying platform, before subsequently displaying a policy-violating ad linking users to a different website.[70] The Russian Doppelganger operation used a variation of this technique to run Meta ads at scale. Ad cloaking requires requisite software and verified accounts, as well as the sharing of techniques, all of which can be acquired through black-hat marketing forums.[71]

Illicit data services can also play a critical role in enabling targeting by providing selectors and other data on target populations. Data breaches available on messaging applications and clear and dark web forums, can provide threat actors with affordable or even free datasets including phone numbers, email addresses, names, account usernames, and much more. This data can then be used to target individuals through SMS, phone call, direct message, paid advertisement, or other channels. Such information can enable targeting of individuals at scale, as well as the targeting of senior-ranking individuals, primarily by exploiting the existing criminal markets for data that are particularly rampant in authoritarian countries such as

---

[68] Gundars Bergmanis-Korāts and Tetiana Haiduchyk, "Social Media Manipulation for Sale: Experiment on Platform Capabilities to Detect and Counter Inauthentic Social Media Engagement," NATO Strategic Communications Centre of Excellence, November 4, 2024.
[69] Poppy McPherson and Karen Lema, "How China Waged an Infowar Against US Interests in the Philippines," Reuters, October 6, 2025.
[70] HUMAN, "What Is Ad Cloaking?" n.d.
[71] BlackHatWorld, "Cloaking - How I Cloak My Google Ads To Get Them Approved," May 5, 2025.

Russia and China.[72] While effective for intelligence and selector-gathering, breached data is less useful for account takeover due to multifactor authentication requirements, difficulty in simulating user sessions, and other protection measures employed by online platforms.

Infostealer logs are a comparatively new source of information that solve this problem. Infostealers are a type of malware that targets a specific device instead of an online service or database. The victim is most commonly infected with the malware after downloading malware in other content, such as pirated media, and is often unaware that their device has been compromised. The infostealer malware then exfiltrates substantial amounts of data from the infected device, including information stored in browsers—such as passwords, cookies, and browsing history—as well as data from local applications, files, and device-specific information such as the operating system and device type. This enables the operator to utilize this information to target privileged accounts and compromise networks.[73] There are multiple possible implementations of this capability in the context of influence operations, such as targeting administrator accounts to deface websites, deploying ransomware on a network for psychological effect, or even simply taking over key social media accounts. Although there are currently no documented examples of infostealers being used for influence operations, their key role in data breaches must be taken into account.

The cybercrime underground has developed offensive tooling and services as well. Distributed denial-of-service (DDoS), or "stresser" services, can be rented at affordable prices. DDoS attacks can serve multiple purposes, such as taking down competitor websites and general vandalism, and in recent years have also been used by pro-state and hacktivist groups for disruption and psychological effect.Groups such as Anonymous Sudan[74] and NoName05716[75] can set up the infrastructure needed by utilizing infected devices or by renting servers to route massive amounts of traffic to their targets. These groups can use this infrastructure for their own operations, rent them out to other actors, or both.

Ransomware is another capability available through the cybercrime underground. Typically used for financial gain, ransomware developers license out the use of their malware to affiliates in exchange for a cut of the profits. This same type of operation can also be used to influence or elicit fear in target audiences, as demonstrated by Iranian actors targeting Israel. This practice is not entirely novel. Pay2Key, which the FBI has identified as an Iranian ransomware operation

---

[72] Pjotr Sauer, "'All Brakes Are Off': Russia's Attempt to Rein In Illicit Market for Leaked Data Backfires," *The Guardian*, December 26, 2025; Kyla Cardona and Ashley Allocca, "'Pantsless Data': Decoding Chinese Cybercrime TTPs," SpyCloud, February 26, 2024.

[73] Australian Cyber Security Centre, "The Silent Heist: Cybercriminals Use Information Stealer Malware to Compromise Corporate Networks," September 2024.

[74] Cloudflare, "What is Anonymous Sudan," n.d.

[75] Europol, "Global Operation Targets NoName05716 Pro-Russian Cybercrime Network," press release, July 16, 2025.

used for influence purposes,[76] has been active since 2020.[77] Pay2Key resumed its activity in mid-2025 during the Israel-Iran war, offering a discount to operators who used their ransomware to target Israeli companies.[78] Other threat actors, such as Qilin, have used a similar modus operandi to target Israeli hospitals.[79] Recent leaks involving Iranian threat actor APT 35 have exposed the scale of this methodology: as per the leaked documents, APT 35 targeted over 300 Israeli websites with ransomware, seeking to then "weaponize the ensuing media exposure."[80]

Other offensive tooling can also be obtained online for combined cyber and influence operations. APT Iran, a Telegram channel affiliated with the IRGC-linked threat actor CyberAv3ngers, offered an offensive framework tool targeting operational technology (OT) systems for sale through online forums.[81] CyberAv3ngers has previously carried out multiple attacks against critical infrastructure and OT systems for psychological effect, such as targeting water systems in the United States.[82] APT Iran has also utilized ransomware software developed by other providers in previous cyber-enabled influence operations targeting Israel.[83]

Part 3: Criminality in the Context of Global Conflict: Closing the Democratic Response Gap

Part 2 of this paper has shown that the range of capabilities and services that cybercriminal infrastructure now affords threat actors working with or on the behalf of authoritarian states has fundamentally outpaced current counter-cyber and influence operation frameworks — rendering existing efforts unlikely to meaningfully curb either the capacity to exert malign influence or the ability to execute attacks on critical national infrastructure. This gap is particularly urgent to address at the present moment: as international competition intensifies and cybercriminal services become ever cheaper, adversarial states are increasingly likely to rely on these options.

As global conflicts intensify, conceptual divergences between authoritarian and liberal-democratic regimes are generating response deficits in the latter. Western liberal democracies draw distinctions between different types of cyber threat and between the state and non-state actors who conduct them; authoritarian regimes rarely make such distinctions. Authoritarian

---

[76] America's Cyber Defense Agency, "Iran-based Cyber Actors Enabling Ransomware Attacks".

[77] ClearSky Cyber Security, "Pay2Kitten: Pay2Key Ransomware – A New Campaign by Fox Kitten," December 2020.
[78] Pierluigi Paganini, "Iranian Group Pay2Key Ramps Up Ransomware Attacks Against Israel and US with Incentives for Affiliates," SecurityAffairs, July 9, 2025.
[79] Nevo Trabelsi, "The Mystery Behind the Cyberattack on Shamir Medical Center: Why Were the Hackers' Demands Removed?" *Globes*, October 8, 2025.
[80] Hamid Kashfi (@hkashfi), "Established footholds in excess of 300 web sites and corporate networks to conduct ransomware attacks and weaponize the ensuing media exposure." X, October 10, 2025.
[81] Lab52, "Black Industry: IRGC-Linked Offensive OT Framework," January 28, 2026
[82] Cybersecurity and Infrastructure Security Agency et al., "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities," advisory AA23-335A, December 1, 2023 (revised December 18, 2024).
[83] Ari Ben Am, "VirusBearSparrow," Memetic Warfare (newsletter), July 28, 2025.

states do not separate attacks on critical infrastructure from influence efforts — they operate in environments of reduced accountability and take a broadly consequentialist approach in which ends justify means. As a result, they deploy whichever actors and tools prove most effective, including groups and individuals who commit cyber-dependent and cyber enabled crimes. In the context of influence operations and hybrid sabotage, reliance on criminal and cybercriminal actors recruited and compensated through digital means is particularly attractive to authoritarian regimes for two reasons: it reduces costs and increases plausible deniability.

Artificial intelligence further enhances the attractiveness of cybercriminal infrastructure by making the criminal supply chain simultaneously harder to detect and cheaper to scale.The CrowdStrike 2026 Global Threat Report documents an 89 percent year-over-year increase in threat actors using AI. The report describes AI use for reconnaissance, credential theft, and evasion of detection.[84] The result is a high tempo of operations conducted against target states at a fraction of their previous cost.

Meanwhile, liberal democracies are failing to recognize the full scope of the threat and are lagging in providing sustained and disruptive responses. Western governments have acknowledged the expansion of influence activity but have yet to fully account for the structural and economic logic driving it. In focusing on the visible architecture of influence operations, they risk overlooking the broader ecosystem that sustains them. Conceptual confusion and terminological imprecision continue to steer counter-measures toward broadly similar solutions, centered on increasing the costs for foreign actors engaging in these operations. However, without addressing the cybercriminal infrastructure that enables them, liberal-democratic responses are projected to remain structurally insufficient.

Infrastructure for cyber and influence operations encompasses the foundational capabilities, software, services, and entities that enable an operator to carry out an operation either partially or completely. Targeting cybercriminal infrastructure, in addition to prebunking, debunking, and longer-term investments in media literacy and societal resilience, confers several unique additional benefits.

First, the infrastructure used is frequently overtly illegal or acquired through illegal means. This illegality neatly bypasses questions of content moderation or the policing of free speech, enabling democratic states to target cybercriminal activity and infrastructure providers using the full range of tools available to them. National police forces, for example, may collaborate with partner states and private companies to conduct takedowns — as Google and its partners did in taking down the residential proxy provider IPIdea.[85] In May 2026, Dutch financial enforcement authorities seized approximately 800 servers from WorkTitans B.V., a hosting provider that was covertly operating as a rebranded, sanctioned, Russian-linked company

[84] CrowdStrike, “2026 Global Threat Report,” February 24, 2026.
[85] Google Threat Intelligence Group, “No Place Like Home Network".

providing infrastructure for Iranian cyber espionage groups.[86] Three Iranian threat actors — MuddyWater, Agrius, and Nimbus Manticore — were all found using WorkTitans servers as their command-and-control backbone, meaning a single law enforcement action simultaneously disrupted multiple active espionage campaigns.[87]

The criminal and foreign nature of these providers also empowers democracies to deploy capabilities that could not be used against on-platform behavior. Offensive cyber operations may also be employed. The US CYBERCOM operation targeting the Russian Internet Research Agency ahead of US elections is an instructive early example of this approach.[88] Other methods targeting key nodes or capabilities — particularly during vulnerable periods such as elections — could be deployed effectively against foundational infrastructure, such as bulletproof hosting services or ransomware developers.

Furthermore, treating influence operations holistically as a threat vector and focusing on high-impact infrastructure incentivizes multiple ministries and agencies within any given country to engage. Foreign ministries can apply political pressure on states in which cybercrime is endemic, reframing the issue as an international crime problem. This approach may help to bypass geopolitical sensitivities and garner support from third countries, international organizations, and international law enforcement bodies that can be deployed against international providers.

Finally, focusing on infrastructure is both cost-effective and high-impact — an important consideration at a time of heightened threats and constrained budgets in Western democracies. While many counter-disinformation initiatives have been cut, moving 'left of post' enables states to target the high-value vendors and capabilities that serve as force multipliers across all types of operations at significantly lower cost. Taking down a residential proxy service or bulletproof hosting provider serving multiple threat actors across multiple states is considerably more cost-effective than reactive methods such as scanning the internet for signs of inauthentic activity. It also generates additional security benefits, including mitigation of broader cybercrime threats.

Conclusions

The contribution of cybercriminal activity to adversarial influence operations is foundational: it provides the tools, functions, and services required to run operations online at scale. Without this infrastructure, the ability of adversarial actors to construct ecosystems of influence assets would be significantly impaired, and such operations would hold little advantage over ordinary organic online activity. These contributions include, but are not limited to, payment capabilities, browsing software, server infrastructure, account procurement and online entity acquisition, and engagement services. Any degradation of this dynamic would substantially

[86] Check Point Team, "The Server Seizure That Affects Iran's Cyber Operations," Check Point, June 1, 2026.
[87] Ibid.
[88] Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 26, 2019.

impair the capacity of adversarial actors to run and sustain scaled operations over a medium to long period of time. Incorporating cybercriminal infrastructure into the analytical frame demands a reconceptualization of the landscape in which influence operations function — one in which diverse actors operate within demand incentives and supply constraints rather than within a state-directed chain of command.

The reconceptualization we call for requires a deeper understanding of the relationships between cybercriminal ecosystems and state threat actors. Although connections between the cybercriminal ecosystem and threat actors are becoming more visible, this ecosystem is separate from and not reliant on nation-state threat actors. State actors did not build the cybercriminal ecosystem that underwrites their influence efforts; rather, they provide it protection and use it as needed.

This dynamic has two main corollaries. First, the infrastructure is self-renewing. Disrupting a specific actor or campaign does not degrade the underlying ecosystem, which continues to operate driven by financially motivated demand. Only by targeting capabilities near the apex of the pyramid of pain, which are less cost-effective to reconstitute, does disruption impose meaningful and lasting friction. Second, the threat will not plateau. Artificial intelligence has reduced, and will continue to reduce, the cost of each link in the cybercriminal supply chain, widening the response gap between liberal democracies and their adversaries.

The market-disruption approach advanced here complements rather than replaces existing counter-influence efforts. Prebunking, media literacy, and long-term societal resilience are still components of any counter-influence strategy, but they should be tail-end efforts. What is currently underinvested is disruption of the supply and enabling side — the fungible, commercially available infrastructure that powers influence operations. Closing that gap requires institutional frameworks, cross-sector partnerships, and legal authorities capable of acting against it systematically rather than episodically. The authoritarian state actors that deploy these operations draw no distinction between their criminal, cyber, and influence instruments. Liberal democracies can adapt to this reality and adopt a proactive posture not only to more effectively defend against hostile foreign interference, but also to degrade the capabilities and infrastructure of their adversaries.

Recommendations

First, democracies must reframe their perception of the problem. Influence operations and foreign interference are only one facet of a broader spectrum of hybrid threats—comprising cybercrime, espionage, sabotage, and others—that must be analyzed holistically. Most democracies still treat these threats as siloed, obstructing the sharing of intelligence, technology, and capabilities across state bodies. The adversary rarely respects these distinctions: the same infrastructure, providers, and personnel service criminal, espionage, and influence activity interchangeably. Microsoft's Digital Crimes Unit and Google's threat-disruption efforts are instructive examples of cross-functional teams that combine legal, technical, and intelligence measures against adversarial infrastructure. Building on this model, law enforcement, intelligence agencies, and foreign ministries should establish joint task forces

to investigate, share information, and coordinate countermeasures in cooperation with Interpol, counterpart task forces abroad, and global technology companies. These partnerships should also develop the protocols and shared technology needed to defend high-value targets, such as elections, proactively rather than reactively.

Second, democracies should recalibrate their diplomatic response. States do not employ the full breadth of measures available to them. Democracies could direct their diplomatic corps to pressure governments that shelter or abet cybercriminals, through measures such as cancelling visa-on-arrival privileges for their nationals, suspending economic or technological cooperation, and imposing targeted sanctions. Pressure should also be applied through joint international bodies such as the United Nations, while recognizing that primary state sponsors often possess the leverage to blunt action in those same forums, making coalitions of like-minded states a more reliable mechanism.

Third, democracies should enlist their legal apparatuses against cybercriminal infrastructure and its enablers. States may employ lawfare against service providers, including supporting their private-sector victims in civil suits, seizing assets located outside the host country, filing additional indictments, pursuing extradition, and closing existing legal loopholes. Coordinated multi-jurisdictional action raises the cost to operators who currently exploit the gaps between national legal systems.

Fourth, democracies should target the shared service layer rather than individual campaigns. Foreign interference and cybercrime run on a commercial supply chain of reusable infrastructure: bulletproof hosting, residential proxy and VPN providers, SMS and phone-verification services, aged-account and access brokers, uncooperative registrars, and beyond. Because these chokepoints are shared across criminal, espionage, and influence clients, degrading a single provider disrupts many downstream actors at once. Democracies should map this ecosystem and prioritize chokepoints by the number of operations they service by building standing capabilities to follow fingerprint and track actors across types of infrastructure, monitoring registrars, resellers, and autonomous systems, and enabling quick action. This requires the targeting discipline to act on malicious providers without indiscriminately disrupting the legitimate co-tenants that often share their address space.

Fifth, democracies should strangle the financial infrastructure that sustains these services. Adversarial infrastructure must be financed, and the payment rails are themselves targetable infrastructure. The crypto exchanges that launder proceeds, the payment processors, and the money-mule networks are identifiable and disruptable; OFAC sanctions against Suex and Garantex, alongside FinCEN's action against Bitzlato, are key first steps.89Sanctioning and de-banking the providers that monetize this ecosystem degrades the business model more durably than seizing a replaceable server.

---

89 U.S. Department of the Treasury, "Treasury Takes Robust Actions to Counter Ransomware," September 21, 2021; U.S. Department of the Treasury, "Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex," April 5, 2022; Financial Crimes Enforcement

Sixth, democracies should degrade and manipulate adversary infrastructure rather than merely seizing it, including its underlying trust substrate. Takedowns are reactive and quickly reconstituted. A more innovative posture treats hostile infrastructure as a persistent target to be degraded and rendered unreliable, raising operating costs and eroding the trust between providers and their clients. Pursuant to a rigorous legal framework, this could include sinkholing and persistent re-infiltration of botnets and command-and-control nodes, corrupting shared resources such as proxy pools and account inventories so they become unreliable to buyers, and selectively manipulating rather than destroying infrastructure to feed adversaries false signals about what has been compromised. The same logic extends to the reputation layer on which this economy depends: the forums, vouching systems, and escrow services that let providers and clients transact with strangers. Compromising escrow, exposing or impersonating trusted brokers, and seeding distrust into vouching systems increases friction across the entire market, turning the adversary's own tradecraft against the infrastructure that sustains them.

Network, "FinCEN Identifies Virtual Currency Exchange Bitzlato as a 'Primary Money Laundering Concern' in Connection with Russian Illicit Finance," January 18, 2023.