A new and better quiet option? Strategies of subversion and cyber conflict

Journal Article

Author(s):
Maschmeyer, Lennart

Publication date:
2022

Permanent link:
https://doi.org/10.3929/ethz-b-000561763

Rights / license:
Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International

Originally published in:
The Journal of Strategic Studies 46(3), https://doi.org/10.1080/01402390.2022.2104253

JOURNAL OF STRATEGIC STUDIES
2023, VOL. 46, NO. 3, 570–594
https://doi.org/10.1080/01402390.2022.2104253

Routledge
Taylor & Francis Group

ARTICLE

A new and better quiet option? Strategies of subversion and cyber conflict

Lennart Maschmeyer

Center for Security Studies, ETH Zurich, Zurich, Switzerland

ABSTRACT
Theorizing on cyber conflict has moved from warfare to conflict short of war, but strategic thought has not kept pace. This article argues cyber conflict is subversive, builds on intelligence scholarship to identify strategies of subversion, and examines their applicability in cyber conflict. It distinguishes three subversive strategies: manipulation, erosion and overthrow. The analysis shows cyber operations can only implement one of these strategies (erosion), indicating they offer less strategic value than traditional counterparts. Accordingly, although cyber operations offer superior scale, I argue their scope of influence is more limited. Finally, the article discusses strategic implications and identifies possible counterstrategies.

KEYWORDS Cybersecurity; covert operations; subversion; strategy; cyber conflict

States now routinely use cyber operations to attain strategic advantages. Yet what strategies enable the achievement of which goals through these instruments still remains unclear. In fact, the very mode of conflict involved is contested. Early theorizing conceived of cyber conflict as a new form of war.[1] Theorists accordingly derived offensive and defensive strategies from the study of war, building on offense-defense theory and nuclear deterrence.[2] Yet in practice cyber conflict has beenlow in intensity, remaining below the threshold of armed conflict.[3] Strategic thought on warfare thus promises limited insights. Accordingly, a current wave of scholarship suggests, cyber

CONTACT Lennart Maschmeyer lmaschmeyer@ethz.ch Haldeneggsteig 4 8092 Zürich Switzerland

[1] John Arquilla and David Ronfeldt, 'Cyberwar Is Coming!', *Comparative Strategy* 12/2 (1 Apr 1993), 141–65, doi:10.1080/01495939308402915; Gary McGraw, 'Cyber War Is Inevitable (Unless We Build Security In)', *Journal of Strategic Studies* 36/1 (Feb. 2013), 109–19, doi:10.1080/01402390.2012.742013; John Stone, 'Cyber War Will Take Place!', *Journal of Strategic Studies* 36/1 (2013), 101–8. doi:10.1080/01402390.2012.730485.

[2] William J. Lynn, 'Defending a New Domain', *Foreign Affairs*, 2010. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain; Joseph S. Nye, 'Nuclear Lessons for Cyber Security?', *Strategic Studies Quarterly* 5/4 (Winter 2011), 18–38.

[3] Jason Healey and Karl Grindal (eds.), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association 2013); Jon R. Lindsay, 'Restrained by Design: The Political Economy of Cybersecurity', *Digital Policy, Regulation and Governance* 19/6 (26 July 2017), 493–514. doi:10.1108/DPRG-05-2017–0023.

conflict occupies a new strategic space where actors can pursue unprecedented strategic gains in conflict short of war by leveraging the vast scale, speed and ease of anonymity that cyberspace enables.[4] One strand of this theorizing focuses on the importance of persistence.[5] Persistence in the offense, it predicts, allows actors to achieve cumulative gains that can shift the balance of power.[6] Conversely, through persistent engagement of such offenders, defenders can deny these gains and impose friction.[7] The United States Cyber Command has adopted the key tenets of this strategy.[8] This is a welcome theoretical and strategic innovation.

However, I argue that just like cyberwar theorists misjudged the operational characteristics and strategic value of cyber operations, current theories of conflict short of war risk building on similarly flawed assumptions. Rather than a new space of competition, a growing body of research shows cyber conflict has key parallels to intelligence contests.[9] In particular, recent work highlights the mechanism of exploitation cyber operations rely upon reveals their nature as instruments of subversion – which offers great strategic promise but provides limited value in practice due to significant operational constraints.[10] Prevailing expectations about a new strategic space focus on the promise, neglecting the constraints. Strategic thought must focus not only on what is theoretically possible, however, but also on what is practically feasible. Here intelligence scholarship on subversion promises key insights for strategic analysis and evaluation.

Building on this literature, this article identifies strategies of subversion, evaluates their efficacy and examines their feasibility in cyber conflict. I outline three distinct strategies. *Manipulation* aims to manipulate government policy, either through exploitation of government or influential political organizations,

[4] Lucas Kello, *The Virtual Weapon and International Order* (Yale: Yale UP, 2017); Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, Massachusetts: Harvard UP 2020); Richard J. Harknett and Max Smeets, 'Cyber Campaigns and Strategic Outcomes', *Journal of Strategic Studies* (4 Mar. 2020), 1–34, doi:10.1080/01402390.2020.1732354.

[5] Michael Fischerkeller and Richard J. Harknett, 'Cyber Persistence Theory, Intelligence Contests and Strategic Competition', Institute for Defense Analysis (June 2020), https://apps.dtic.mil/sti/pdfs/AD1118679.pdf.

[6] Harknett and Smeets, 'Cyber Campaigns and Strategic Outcomes'.

[7] Michael P. Fischerkeller and Richard J. Harknett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation', *The Cyber Defense Review* (2019), 267–87. doi:10.2307/26846132.

[8] US CYBERCOM, 'Achieve and Maintain Cyberspace Superiority – Command Vision for US Cyber Command', Apr. 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018pdf?er=2018-06-14-152556-010.

[9] Erik Gartzke and Jon R. Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', *Security Studies* 24/2 (3 Apr. 2015), 316–48. doi:10.1080/09636412.2015.1038188; Aaron Franklin Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making* (Athens, GA: University of Georgia Press 2016). http://muse.jhu.edu/book/45365; Joshua Rovner, 'Cyber War as an Intelligence Contest', *War on the Rocks*, 16 Sept. 2019. https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

[10] Lennart Maschmeyer, 'The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations', *International Security* 46/2 (25 Oct. 2021), 51–90. doi:10.1162/isec_a_00418.

or indirectly by swaying public opinion. *Erosion* strives to undermine an adversary's sources of strength by eroding public trust, exacerbating societal tensions and sabotaging institutions and infrastructure. *Overthrow* attempts to replace a regime with one aligned with the subverter's interests by mobilizing and supporting opposition groups. I sort these strategies according to their ascending potential to shift the balance of power. However, greater strategic impact also brings greater operational challenges, thus raising the risk of failure.

Examining the feasibility of implementing these strategies through cyber operations produces surprises. Unsurprisingly, considering the scale of the Internet, cyber operations enable a greater scale of intrusion compared to traditional subversion. However, the analysis shows the scope of their reach, and thus the scope of *manipulation* they can achieve, to be more limited. Furthermore – and counterintuitively, considering prevailing expectations of conflict at the 'speed of light'– cyber operations are relatively slow. Consequently, they are most suited to the *erosion* strategy. It offers an attractive option to weaken an adversary without facing the risks and costs of war, in line with current expectations about cumulative shifts in the balance of power. However, I show this strategy faces two important limitations. First, it requires significant operational capacity and resources. Contrary to prevailing expectations of the low barriers to entry in cyber conflict, these requirements likely reserve the strategy for the largest and most advanced states. Second, even with these requirements fulfilled, its chance of success is very limited due to the operational challenges of subversion. Concerning the *overthrow* strategy, the analysis shows cyber operations are incapable of independently implementing it – further underlining their limitations. The article concludes with a discussion of the consequences for world politics and shows why drawing on intelligence studies enables more effective strategies than a universal focus on persistence by countering specific operation and effect types.

This article makes three contributions. First, it furthers strategic thought on cyber conflict by identifying three distinct strategies and evaluating their relative efficacy. Second, through its investigation of the historical parallels between cyber conflict and intelligence operations, it adds to the understanding of the strategic role of both cyber operations and subversive covert operations. Third, by comparing the relative advantages and disadvantages of cyber operations and their historical counterparts in implementing these three strategies, the article refines our understanding of how technological change has impacted competition short of war. Finally, these insights provide a foundation for future strategy development.

Strategic thought on cyber conflict

Cyber conflict refers to the use of cyber operations by actors in security competition and conflict in pursuit of political goals. Cyber operations exploit information technologies embedded in societies to produce desired outcomes.[11] Early scholarship conceived of cyber conflict as warfare, hence early strategic thought built on theories of war. In offense, scholars posited, strategic 'cyber strikes' would provide independent strategic value at low risk.[12] Alternatively, cyber operations could also complement force, increasing the latter's effectiveness.[13] Because these characteristics favor the offense, scholars identified deterrence as the best strategy to avoid escalation.[14] The United States adopted a strategy of cyber deterrence in 2011.[15]

In practice, however, cyber conflict has looked nothing like this. There have been no strategic strikes and no escalation.[16] Empirical studies instead document the irrelevance of cyber operations in war.[17] Yet actors frequently deploy them.[18] Actual cyber conflict, however, has been marked by consistently low intensity.[19] Moreover, there is little evidence that deterrence explains this lack of escalation. Rather, the causes are operational. A growing body of research shows cyber operations are ineffective at force projection or coercion.[20] Accordingly, scholars and policy-makers now widely

[11] Outcomes can include both the exfiltration of information as well as active effects on the target, i.e., manipulation of data, disruption or damage. This argument focuses on the latter.

[12] Lynn, 'Defending a New Domain'; Nye, 'Nuclear Lessons for Cyber Security?'; James J. Wirtz, 'The Cyber Pearl Harbor', in *Cyber Analogies* (Monterey, CA: Naval Postgraduate School 2014).

[13] Max Smeets, 'The Strategic Promise of Offensive Cyber Operations', *Strategic Studies Quarterly*, 18/3 (Fall 2018); Jon R. Lindsay and Erik Gartzke, 'Coercion through Cyberspace: The Stability-Instability Paradox Revisited' in *The Power to Hurt: Coercion in Theory and in Practice*, ed. Peter Krause (New York: Oxford UP 2018).

[14] Richard L. Kugler, 'Deterrence of Cyber Attacks', in *From Cyberspace to Cyberpower: Defining the Problem* (Washington, DC: Potomac Books 2009), 309–42; Will Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly* 4/3 (Fall 2010), 102–35.

[15] DoD, 'Strategy for Operating in Cyberspace', 10 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf; The White House, 'International Strategy for Cyberspace', 12 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[16] Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35/1 (Feb. 2012), 5–32. doi:10.1080/01402390.2011.608939; Erik Gartzke, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security* 38/2 (2013), 41–73.

[17] N. Kostyuk and Yuri M. Zhukov, 'Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?', *Journal of Conflict Resolution* 63/2 (2017), 317–47. doi:10.1177/0022002717737138; Aaron F. Brantly, N. Cal, and D. Winkelstein, 'Defending the Borderland', Report (Army Cyber Institute, 1 Dec. 2017). https://vtechworks.lib.vt.edu/handle/10919/81979.

[18] Specops, 'The Countries Experiencing the Most "Significant" Cyber-Attacks', Specops Software, 9 July 2020. https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/.

[19] Healey and Grindal, *A Fierce Domain*; Lindsay, 'Restrained by Design'.

[20] Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies* 22/3 (2013), 365–404. doi:10.1080/09636412.2013.816122; Rebecca Slayton, 'What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment', *International Security* 41/3 (Jan. 2017), 72–109. doi:10.1162/ISEC_a_00267; Maschmeyer, 'The Subversive Trilemma'.

agree cyber deterrence falls short both as a theory and as a strategy.[21] In short, cyberwar theories and associated strategic thought offer at best limited utility.

Theorizing has since moved on to conflict short of war, but strategic thought has not kept pace. A new body of scholarship proposes cyber operations offer a new instrument to achieve strategic gains in conflict short of war.[22] In offense, it suggests, by persistently deploying cyber operations actors can shift the balance of power without using force.[23] As discussed, an emerging defensive strategy prescribes 'persistent engagement' to deny adversaries these gains. Yet, I argue, this strategy rests on similarly flawed assumptions as its predecessor. The underlying theory of 'cyber persistence' suggests the interconnected nature of cyberspace places actors in 'constant contact', necessitating persistent engagement to prevail.[24] In practice, however, interconnectedness and constant contact are not given structural conditions, but actor-specific variables.[25] Consider the Stuxnet operation, one of the most analyzed cases of cyber conflict that involved damage to nuclear enrichment centrifuges. Crucially, the target computer systems were not connected to the Internet. Rather, the operation required local human agents who transferred the malicious software to the facility.[26] In other words, no matter how persistent the actor had been, without a means to connect to the target system, the operation had no chance of success.

Accordingly, persistence is important, but only constitutes one determinant of success. Because victims can neutralize means of exploitation upon discovery, for example, secrecy and its maintenance are as, if not more, important.[27] Consequently, cyber operations often aim to produce effects *without* engaging the adversary. Rather, they produce outcomes by exploiting vulnerabilities in computer systems to make these systems behave in unexpected ways, creating detrimental effects against an adversary indirectly and *before* the latter can detect and neutralize the exploitation.[28] Focusing only on persistence risks neglecting these other determinants of success and provides an opening to adversaries who leverage their advantages.

[21] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND 2009); Michael P. Fischerkeller and Richard J. Harknett, 'Deterrence Is Not a Credible Strategy for Cyberspace', *Orbis* 61/3 (1 Jan. 2017), 381–93. doi:10.1016/j.orbis.2017.05.003; Brad D. Williams, 'Nakasone: Cold War-Style Deterrence "Does Not Comport to Cyberspace"', *Breaking Defense* (blog), 4 Nov. 2021. https://breakingdefense.sites.breakingmedia.com/2021/11/nakasone-cold-war-style-deterrence-does-not-comport-to-cyberspace/.

[22] Kello, *The Virtual Weapon and International Order*; Buchanan, *The Hacker and the State*; Harknett and Smeets, 'Cyber Campaigns and Strategic Outcomes'.

[23] Harknett and Smeets, 'Cyber Campaigns and Strategic Outcomes'.

[24] Fischerkeller and Harknett, 'Cyber Persistence Theory, Intelligence Contests and Strategic Competition'.

[25] Lindsay and Gartzke, 'Coercion through Cyberspace: The Stability-Instability Paradox Revisited'.

[26] Lindsay, 'Stuxnet and the Limits of Cyber Warfare', 381.

[27] Jon Erickson, *Hacking: The Art of Exploitation* (San Francisco: No Starch Press 2003), 320.

[28] Thomas Dullien, 'Weird Machines, Exploitability, and Provable Unexploitability', *IEEE Transactions on Emerging Topics in Computing* 8/2 (Apr 2020), 391–403. doi:10.1109/TETC.2017.2785299.

Similarly, the presumed novelty of the strategic space occupied by cyber operations does not withstand historical comparison. States have long had a 'quiet option' at their disposal to pursue strategic gains that went beyond traditional diplomacy but fell short of warfare: covert operations.[29] Accordingly, a growing set of scholarship emphasizes the parallels between cyber conflict and intelligence contests.[30] Specifically, recent literature has highlighted the subversive nature of cyber conflict.[31] Intelligence scholarship on subversion thus promises key insights to further strategic thought on cyber conflict, as next section will show.

Strategies of subversion

Strategically, subversion offers an alternative to diplomacy that promises similar results to warfare at lower costs and risks. Subversion is an instrument in covert operations, defined as intelligence operations that actively interfere in adversary affairs (rather than passively collecting information). Importantly, covert operations come in many varieties.[32] Some involve violence and force, namely assassination and secret wars.[33] Subversion, in contrast is non-military, relying on the exploitation of vulnerabilities in adversary systems to manipulate the latter into producing outcomes not expected or intended by their designers or participants.[34] It has two key characteristics: it is secret and indirect. Traditionally, subversion uses spies to infiltrate societies, organizations or groups (i.e., social systems of rules and practices) and establish influence.[35] Actors then use this influence to secretly manipulate these systems towards producing desired outcomes against adversaries. Subversive operations produce outcomes through two types of agents: spies and the individuals, groups and organizations they have established influence over. An agent in this context is defined as "a person or thing that takes an active role or produces a specified effect".[36] Subversive

[29] James Callanan, *Covert Action in the Cold War: US Policy, Intelligence and CIA Operations* (New York: I.B. Tauris 2009); Loch K. Johnson, *The Third Option: Covert Action and American Foreign Policy* (Oxford: Oxford UP 2022).

[30] Gartzke and Lindsay, 'Weaving Tangled Webs'; Brantly, *The Decision to Attack*, chap. 2; Rovner, 'Cyber War as an Intelligence Contest'.

[31] Maschmeyer, 'The Subversive Trilemma'.

[32] Loch K. Johnson, 'On Drawing a Bright Line for Covert Operations', *The American Journal of International Law* 86/2 (1992), 284–309. doi:10.2307/2203235.

[33] Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton, NJ: Princeton UP 2018).

[34] Paul W. Blackstock, *The Strategy of Subversion: Manipulating the Politics of Other Nations*. (Chicago: Quadrangle Books 1964), 50; Maschmeyer, 'The Subversive Trilemma', 54.

[35] Blackstock, *The Strategy of Subversion*; Beilenson, *Power Through Subversion*.

[36] Definition in the Oxford Dictionary (2021).

agents can cause manifold effects: manipulating policy, conducting sabotage, causing economic disruption, undermining institutions, mobilizing people and, if needed, arming them.[37]

This non-military instrument of secret statecraft has been notoriously understudied, and, likely as a consequence, analysts and policy-makers have overestimated its effectiveness[38]—just as with cyber operations today.[39] Consequently, it is important to evaluate the strategic value of strategies of subversion. Strategic value in this context refers to the capacity to attain political goals and/or shifts in the balance of power. Although existing literature is scarce and mostly narrative, three distinct strategies can be synthesized. These are not mutually exclusive but can be complementary and cumulative.

Manipulation

The first subversive strategy aims to secretly manipulate adversary policy to align with the sponsor's interests. Actors have long used a wide range of non-military means to influence adversary policy, foremost diplomatic instruments. Subversion is distinct from such general influence, however, because it strives to keep the influence secret – instead exploiting systems within adversary jurisdiction to turn them into covert instruments of the subverting actor's power to manipulate government policy. There are two main means to purse this strategy: spies and propaganda (covert and overt).[40] Spies can infiltrate government itself to manipulate it. A key example is Günter Guillaume, an East German undercover agent who became one of former German Chancellor Willy Brandt's closest advisors during the 1970s.[41] A second pathway involves infiltrating political organizations with sufficient clout to shape government policy – purportedly acting in their own interest, yet in fact carrying out the subverting actor's agenda. The third path towards manipulation targets public opinion. Propaganda is the classic instrument[42] and Radio Free Europe offers a key example of a propaganda channel aimed at populations in the Soviet-controlled parts of Europe. Apart from overt propaganda whose source is known, covert propaganda offers a stealthy subversive alternative. To implement it, undercover spies are again key. One of the KGB's preferred tactics exploited the openness of Western

[37] Johnson, 'On Drawing a Bright Line for Covert Operations'; Blackstock, *The Strategy of Subversion*, 51, 69; Beilenson, *Power Through Subversion*, 80.

[38] Blackstock, *The Strategy of Subversion*, 321.

[39] Maschmeyer, 'The Subversive Trilemma'.

[40] Blackstock, *The Strategy of Subversion*, 69.

[41] Eckard Michels, *Guillaume, Der Spion: Eine Deutsch-Deutsche Karriere* (Berlin: Ch. Links Verlag 2013), 131–50.

[42] Richard H. Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy* (Washington DC: Pergamon-Brassey's 1984), 34.

media to establish ‘agents of influence’ within media outlets who spread disinformation under the mantle of free journalistic expression. The Danish journalist Arne Herlov Petersen offers an example, publishing anti-NATO disinformation, forgeries and even providing KGB funds to opposition groups for ten years until his arrest in 1981.[43]

Manipulation aims to cause a shift in domestic or foreign policy furthering the interests of the sponsor. Accordingly, the KGB’s overarching strategic goal was “to isolate the United States from its friends and allies (especially those in NATO), and to discredit those states which cooperate with the United States”.[44] Manipulation is useful in both peace and war, and has been used in great power competition, in asymmetric power relationships and between middle and small powers.[45] Conditions for success are exploitable vulnerabilities in target governments, political institutions and media outlets, and for manipulation of public opinion to work, sufficient susceptibility of government policy to public opinion. For manipulation of public opinion to produce effects in practice, the propaganda must reach a sufficiently large audience and achieve a sufficient individual effect. Both pose non-trivial challenges in practice.[46] Accordingly, while there is ample evidence of attempted manipulation during the Cold War, evidence of operations causing a measurable impact on relevant policy is scarce.

Erosion

The second strategy of subversion aims to weaken an adversary through a typically slow-burning campaign of sabotage and disruption. The goal is to maintain or achieve a favorable balance of power over the longer term rather than to fulfil a specific short-term objective. As such, it strives to erode the pillars of an adversary’s strength, namely public support for the government, economic and industrial capacity, and, as a riskier option, military capabilities. Propaganda remains relevant to undermine public support. To erode economic and industrial capacity, spies are more useful. The KGB ‘Illegals’, undercover spies with carefully constructed cover identities provide an example. They established positions of influence in key institutions across the West, developed plans to sabotage critical infrastructure, attempted to trigger crop failures and even prepared arms caches to use in case of military escalation.[47]

[43] Ladislav Bittman, *The KGB and Soviet Disinformation: An Insider’s View* (Washington DC: Pergamon-Brassey’s 1985), 87.

[44] Shultz and Godson, *Dezinformatsia*, 40.

[45] Blackstock, *The Strategy of Subversion*; Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, Peacekeeping* (London: Faber 1971); William C. Wohlforth, ‘Realism and Great Power Subversion’, *International Relations* 34/4 (1 Dec. 2020), 459–81. doi: 10.1177/0047117820968858.

[46] Lennart Maschmeyer, ‘Digital Disinformation: Evidence from Ukraine’, CSS Analysis No. 278, Feb. 2021. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse278-EN.pdf.

[47] Christopher M. Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*, 1st ed. (New York: Basic Books 1999).

The aim was to weaken the Western alliance from within. Another tactic in the pursuit of this strategy is to undermine cohesion, efficiency and effectiveness in targeted institutions, for example by manipulating or disrupting internal communication and management processes. Coincidentally, the CIA predecessor organization Office of Strategic Services, provides detailed instructions of doing so in a 1944 handbook.[48]

This strategy is mainly relevant in great power competition.[49] Because there is no clear goal, but rather an effort to maintain or alter the balance of power over a longer term, defining success is not as straightforward as in the previous strategy. The best available measure are shifts in public opinion, economic and industrial capacity, and material capabilities. Conditions for success are available vulnerabilities in the targeted state, as well as sufficient organizational capacity and resources to establish the network of spies required to produce effects and maintain it long enough to achieve measurable impacts. The capacity and resources required are significant, and thus typically online available to large states. For example, training illegal agents takes many years, and establishing their cover identities requires additional years of living in target countries.[50] Meanwhile, due to the challenges involved, effects will likely have at best marginal impacts on the balance of power. Hence, in asymmetric power relationships marked by significant power differentials, this strategy is unlikely to produce meaningful advantages to the more powerful side. Nonetheless, having subversive networks opens opportunities to implement strategies one or two over time, thus enabling potentially more significant gains.

Finally, military targeting indicates a potential auxiliary used of this strategy: softening up an adversary to facilitate the use of force. Barron notes how the KGB pursued an ability to "sabotage foreign public utilities, transportation and communications facilities, and other nerve centers in peacetime … to give Soviet rulers the option of immobilizing Western countries through internal chaos during future international crises".[51] These efforts are documented in the Mitrokhin archive, which shows clear efforts by illegals to prepare wartime sabotage of critical infrastructure across NATO.[52] Beilenson similarly talks of 'preparatory subversion' for a "final blow by force".[53]

This auxiliary strategy obviously conflicts with the supposed strategic purpose of subversion as an alternative to the use of force. Accordingly, existing literature is unclear and contradictory on the strategic contexts under which it is useful. In the bipolar competition during the Cold War,

[48] OSS, 'Simple Sabotage Field Manual', 1944.
[49] Wohlforth, 'Realism and Great Power Subversion'.
[50] Andrew and Mitrokhin, *The Sword and the Shield*, 265–91.
[51] John Barron, *KGB: The Secret Work of Soviet Secret Agents* (London: Hodder and Stoughton 1975), 78.
[52] Andrew and Mitrokhin, *The Sword and the Shield*, 468.
[53] Beilenson, *Power Through Subversion*, vii.

the purpose is clear: weakening the adversary without using force as long as possible, but preparing for the outbreak of hostilities to gain advantages if it happens. Yet in other contexts, it is not clear if the success or failure of strategies of subversion can trigger the very use of force its deployment is supposedly intended to avoid. Blackstock suggests that both success *and* failure of subversion can lead to armed intervention. First, he notes that, "when covert operations end in … spectacular failure or are clearly inadequate, the two most likely alternatives open to the aggressor are to call them off or to intervene directly with military action".[54] Yet he then suggests that having established "a degree of covert control over the political and social institutions of the victimized state, the intervening power may openly seize power … frequently involv[ing] the use or threat of military force".[55] Importantly, both examples suggest subversion alone is incapable of establishing full political control within a target state – further underlining its limitations.

Overthrow

The third strategy goes further than manipulation, aiming to overthrow a government. Cold War literature in fact often defines subversion by this goal alone.[56] Spies play a key role in this strategy as well, identifying, contacting and/or infiltrating suitable opposition groups and organizations to coordinate their challenge of the government – and providing material support as needed.[57] There are two ways to implement the overthrow: a public revolution, either peaceful or armed, or a 'palace coup d'etat' where a government faction takes over control internally. To achieve the latter, government infiltration with spies is a key asset. The CIA's Operation TPAJAX offers an example, which aimed to overthrow Prime Minister Mossadegh' government in Iran in 1953 by turning key power holders against him. When this failed, the CIA used an existing network of agents and collaborating proxy groups to instigate a public revolt, forcing Mossadegh to resign.[58] Without such government infiltration, in Guatemala the CIA pursued armed revolt from the start to affect regime change through 1954's Operation PBSUCCESS, training a rebel force to instigate the revolt that removed President Juan Guzmán from office.[59] If successful, this strategy

[54] Blackstock, *The Strategy of Subversion*, 70.

[55] Blackstock, 75–76.

[56] Kitson, *Low Intensity Operations*, 3; Beilenson, *Power Through Subversion*, v.

[57] Blackstock, *The Strategy of Subversion*, chap. 7; Lindsey A. O'Rourke, *Covert Regime Change: America's Secret Cold War* (Ithaca, NY: Cornell UP 2018); Melissa M. Lee, *Crippling Leviathan: How Foreign Subversion Weakens the State* (Ithaca, NY: Cornell UP 2020).

[58] Callanan, *Covert Action in the Cold War*, 115–18.

[59] Callanan, 119–24.

offers the most significant strategic impact by lastingly changing the underlying foreign policy preferences of another government – thereby removing the source of conflict: conflicting preferences.[60]

The strategic contexts for regime change have predominantly been large states aiming to influence smaller states, i.e., asymmetric power relationships between great or middle powers and small powers.[61] It also offers a pivot if manipulation fails to produce the desired outcome, while staying short of armed intervention. Conditions for success are available vulnerabilities within a target government, incomplete sovereignty as well as suitable proxy actors with sufficient capacity to mount a revolution.[62] Moreover, if the latter is not given, expanding the capacity of these proxy actors requires significant organizational capacity and material resources by the sponsor. Only the intelligence agencies of the largest states typically fulfil these requirements.

In line with these constraints, the track record of subversion is decidedly mixed. Its history involves a string of failures across all three strategies. Manipulation operations often had no effect or backfired if discovered,[63] and similarly regime-change operations failed more often than they succeeded.[64] Moreover, even successful operations often fail to reduce the risks of conflict between the parties involved, while raising the probability of civil strife within the target country.[65] As discussed, measuring the success of the erosion strategy is more difficult as it pursues marginal change, yet here a string of failures and abandoned plans in the KGB illegal program attests to its shortcomings.[66] Importantly, analysts and policy-makers have tended to focus on the possibilities rather than the reality of subversion. Consequently, during the early Cold War “the capabilities of the covert operational arm of government were greatly overestimated and early sanguine hopes have been disappointed”.[67] No evidence indicates subversion measurably impacted great power rivalries.[68] There is an obvious parallel to current expectations in cybersecurity, where scholarship is rife with strategic possibilities and

[60] O’Rourke, *Covert Regime Change*, 42.

[61] O’Rourke, 45.

[62] Blackstock, *The Strategy of Subversion*, 158–60; Beilenson, *Power Through Subversion*; O’Rourke, *Covert Regime Change*, 9; Lee, *Crippling Leviathan*, 8–10.

[63] Bittman, *The KGB and Soviet Disinformation*, 98,106,149,153.

[64] O’Rourke, *Covert Regime Change*, 77.

[65] Benjamin C. Denison, ‘Strategies of Domination: Uncertainty, Local Institutions, and the Politics of Foreign Rule’ (University of Notre Dame 2018). https://curate.nd.edu/show/j6731260871; Alexander B. Downes, *Catastrophic Success: Why Foreign-Imposed Regime Change Goes Wrong*, Cornell Studies in Security Affairs (Ithaca, NY: Cornell UP 2021).

[66] Christopher M. Andrew, *The Mitrokhin Archive : The KGB in Europe and the West* (London: Allen Lane 2000).

[67] Blackstock, *The Strategy of Subversion*.

[68] Wohlforth, ‘Realism and Great Power Subversion’, 467.

hypothetical threat scenarios[69] yet empirical evidence of actual strategic impact remains scarce.[70] As the next section will show, strategies of cyber-enabled subversion involve similar limitations.

Strategies of cyber subversion

Like traditional subversion, many expect cyber operations to provide strategic gains without going to war. Richard Harknett and Max Smeets argue that "cyber campaigns and operations can be pivotal in world affairs by independently … supporting the maintenance or alteration of the balance of power … without having to resort to military violence".[71] As with traditional subversion, there is also a tendency to overestimate the strategic value of this instrument by underestimating the operational constraints involved.[72] These constraints are key when considering the capacity of cyber operations to implement established strategies of subversion. As the analysis below will show, perhaps counterintuitively, cyber operations are likely best suited for the strategy of erosion, while facing relatively greater limitations in strategies of manipulation and overthrow.

Manipulation

In theory, cyber operations are clearly capable of implementing the strategy of manipulation. In practice, however, they are more limited in the scope of manipulating government and it is uncertain whether their potential greater scale in manipulating public opinion offsets this limitation. Spies can infiltrate governments directly and build personal relationships providing them 'access to the minds' of targeted individuals.[73] Hence, spies can not only find out what their targets are preoccupied with, but also exploit their personality traits to manipulate their thinking and perception. Cyber operations lack this direct access and interpersonal relationships since they depend on computer systems. It is, of course, possible to attempt to manipulate government officials through forged information spread online – yet such means of manipulation lack the direct personal relationship that has always been a key advantage of human agents. Accordingly, it is unsurprising there are no recorded cases of cyber manipulation comparable to a Günther Guillaume.

[69] M. Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', *International Studies Review* 15/1 (2013), 105–22, 10.1111/misr.12023.

[70] Robert Gorwa and Max Smeets, 'Cyber Conflict in Political Science: A Review of Methods and Literature', preprint (SocArXiv, 25 July 2019), 10.31235/osf.io/fc6sg.

[71] Harknett and Smeets, 'Cyber Campaigns and Strategic Outcomes', 24.

[72] Maschmeyer, 'The Subversive Trilemma'.

[73] Stephen Grey, *The New Spymasters: Inside the Modern World of Espionage from the Cold War to Global Terror* (New York: St. Martin's Press 2015), 126.

Because of the scale of communication networks, and particularly the vast audiences of social media platforms, cyber operations that exploit these networks and platforms promise a way to sway public opinion at unprecedented scale. Indeed, the election meddling campaign targeting the 2016 United States Presidential Election attributed to Russia provides a contemporary example of such cyber-enabled manipulation. By leaking damaging information obtained from compromised email accounts of leading figures in the Democratic party, spreading disinformation via social media platforms and setting up bogus online groups to mobilize individuals towards unrest, this campaign aimed to exploit legitimate functionality of social media networks to turn them into targeted instruments to secretly manipulate voter preference towards the Republican Party. Whether this campaign had a significant effect on voting remains hotly debated, and while a majority of scholars has concluded it did not, some circumstantial evidence does indicate a possible impact on voting outcomes – with significant consequences considering the small margins by which this election was decided.[74] Importantly, however, even those who argue in favor of a measurable effect underline the importance of traditional news media rather than social media in disseminating the leaks that damaged Clinton's standing.[75] Accordingly, Rovner and Moore highlight this was a traditional active measures campaign.[76] Moreover, emerging research on the efficacy of social media disinformation indicates significant shortcomings[77]—contrary to prevailing fears.

Cyber manipulation suits similarly diverse strategic contexts as traditional counterparts. However, the conditions for success are steeper since cyber operations cannot produce the same scope of direct manipulation of government policy through infiltration and thus depend on public opinion. This dependence produces two limitations. First, the less publicly accountable a target government is, the less the potential impact. Second, as their traditional counterparts, cyber manipulation campaigns must reach a sufficiently large audience and produce sufficient individual effects to cause public opinion shifts at the national level. While possible in theory, systematic

[74] Kathleen Hall Jamieson, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President What We Don't, Can't, and Do Know* (New York, NY: Oxford UP 2018); Damian J. Ruck et al., 'Internet Research Agency Twitter Activity Predicted 2016 U.S. Election Polls', *First Monday* 24/7 (30 June 2019). doi:10.5210/fm.v24i7.10107; Dov H. Levin, *Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions* (New York, NY: Oxford UP 2020), 229.

[75] Jamieson, *Cyberwar*, 149–88; Levin, *Meddling in the Ballot Box*, 231; Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Farrar, Straus and Giroux 2020), 382.

[76] Joshua Rovner and Tyler Moore, 'Does the Internet Need a Hegemon?', *Journal of Global Security Studies* 2/3 (1 July 2017), 185. doi:10.1093/jogss/ogx008.

[77] See, for example: Andrew Leber and Alexei Abrahams, 'A Storm of Tweets: Social Media Manipulation During the Gulf Crisis', *Review of Middle East Studies* 53/2 (Dec. 2019), 241–58. doi:10.1017/rms.2019.45; Christopher A. Bail et al., 'Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017', *Proceedings of the National Academy of Sciences* 117/1 (7 Jan. 2020), 243–50. doi:10.1073/pnas.1906420116.

evidence of success in practice remains lacking – reflecting the steep challenges involved. Specifically, it would require evidence of a causal linkage between a manipulation operation or campaign and 1) a government policy change towards the subverter's preferences, 2) a public opinion change towards majority endorsement of the subverter's preferred position, or 3) auxiliary evidence showing a campaign reached an audience of sufficient size to facilitate a public opinion shift.

Erosion

Rather, cyber operations are most suited for the second strategy, slow-burning erosion of adversary strength. Empirical evidence shows cyber operations successfully sabotaging critical infrastructure, causing economic disruption and achieving temporary institutional paralysis. The Stuxnet malware damaged Iranian nuclear enrichment centrifuges,[78] while the hacking group Sandworm used a clever combination of malware and skill to create power blackouts in Ukraine – twice.[79] The NotPetya malware in turn disabled computer systems by encrypting data and spread not only to most businesses in Ukraine, but ultimately to 65 countries, shaving of half a percentage point of Ukraine's GDP and causing billions of dollars of damage.[80] Finally, a string of 'ransomware' attacks, where hackers encrypt and disable systems while demanding a ransom to reverse the encryption, have hit local governments and utilities across the Western world.[81] These types of effects are exactly congruent with the erosion strategy, and emerging strategic thought on the strategy of 'persistent engagement' correctly identifies this erosive and corrosive nature of cyber campaigns and their cumulative effects.[82] However, by focusing on potential rather than feasible outcomes, these theories overestimate its strategic value, and consequently neglect the operational challenges involved – potentially undermining, as I argue further below, the efficacy of a strategy focusing on persistence alone.

[78] Ralph Langner, 'To Kill a Centrifuge', Nov. 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

[79] ESET, 'BlackEnergy Trojan Strikes Again: Attacks Ukrainian Electric Power Industry', *WeLiveSecurity* (blog), 4 Jan. 2016. https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/.

[80] Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, 22 Aug. 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[81] Arielle Waldman, 'FBI: Ransomware Hit 649 Critical Infrastructure Entities in 2021', *SearchSecurity*, 24 Mar. 2022. https://www.techtarget.com/searchsecurity/news/252515076/FBI-Ransomware-hit-649-critical-infrastructure-entities-in-2021.

[82] Kello, *The Virtual Weapon and International Order*, 76; Harknett and Smeets, 'Cyber Campaigns and Strategic Outcomes'; Paul M. Nakasone and Michael Sulmeyer, 'How to Compete in Cyberspace', 17 Mar 2021. https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity; Michael Fischerkeller, 'The Structural and Strategic Imperative: The Need for Persistent Engagement' (IDA, n.d.). https://www.ida.org/research-and-publications/-/media/2e11bf09b5a44cb49e59571704171218.ashx.

First of all, operational success does not guarantee strategic value. For example, although the Stuxnet operation achieved its operational objective of damaging centrifuges, it did not significantly impede Iran's progress towards obtaining nuclear capabilities, and likely cost more to implement than the damage it caused.[83] Similarly, NotPetya's global disruption was most likely accidental, and the result of a control loss rather than strategic calculation[84]–and produced post-hoc costs for Russia as victimized countries imposed punitive sanctions.[85] Finally, ransomware operations are motivated by financial gain, and are typically reversible. Hence, rather than causing long-term erosion in institutional effectiveness, they trigger temporary nuisances. In traditional subversion, agents of influence established in an institution can hollow it out from within, undermining decision and management processes. Cyber operations currently fall short of doing so since most decision and management processes are (still) being carried out by humans rather than computers.

The last point highlights that conditions for success of cyber erosion pose as, if not more, demanding challenges as traditional subversion. Establishing and maintaining exploitation of adversary systems at the scope and scale necessary to achieve strategic impact requires significant organizational capacity and, particularly, highly-skilled labor.[86] As in traditional subversion, only the largest intelligence agencies will have enough of both to attempt this strategy. Even under these conditions, as already discussed, success is uncertain due to the considerable operational challenges involved. Success in this context would mean causing a measurable impact on the balance of power, or on public opinion in a target country (e.g., a gradual loss of trust in the government). Empirical evidence of such success(es) is lacking. On the contrary, there are clear indications Russia's campaign of erosive cyber operations against Ukraine from 2014–2018 failed to measurably contribute to its strategic goals; consequently, we have now, tragically, witnessed Russia revert to the use of force.[87] Nonetheless, because the risks are relatively low – no actor has thus far escalated conflict in response to cyber operations of this type, and wargaming exercises have shown decision-

[83] Lindsay, 'Stuxnet and the Limits of Cyber Warfare'; Slayton, 'What Is the Cyber Offense-Defense Balance?'.

[84] ESET, 'Bad Rabbit: Not-Petya Is Back with Improved Ransomware', 24 Oct. 2017. https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/.

[85] US Treasury, 'Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks | U.S. Department of the Treasury', 15 Mar. 2018, https://home.treasury.gov/news/press-releases/sm0312.

[86] Slayton, 'What Is the Cyber Offense-Defense Balance?'.

[87] Maschmeyer, 'The Subversive Trilemma'; Lennart Maschmeyer and Nadiya Kostyuk, 'There Is No Cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict', *War on the Rocks* (blog), 8 Feb. 2022. https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/.

makers consistently avoid such escalation[88]— even with uncertain value this strategy remains attractive, especially in long-term competition among powerful states. It offers way to keep the enemy on its toes and gain relative advantages without going to war, as small as they might be. Erosion is thus not a replacement for war, but rather a possible means to forestall the outbreak of hostilities.

Because erosion is unlikely to enable decisive shifts in the balance of power, as in traditional subversion its instruments of sabotage, disruption and influence may also be used for an auxiliary strategy of 'softening up' an adversary. Here as well, both success and failure can conceivably entail armed escalation. If an actor deems they have, through a long-term cyber campaign, gained enough of an advantage over an adversary that makes the prospects of using force likely to bring decisive victory, this outcome becomes more probable. While it is a conceivable scenario, the limited strategic impact of cyber operations and campaigns makes it unlikely in most circumstances. Moreover, if cyber campaigns have produced strategic value of such significance, why not continue to rely on them rather than go for the costlier and riskier option of war? An alternative scenario is more likely, where actors fail to stop perceived losses in their relative power compared to a competitor via cyber operations and campaigns, and opt for war as a last resort to curb the competitor's rise before it is too late.

As the above point illustrates, paradoxically, and ironically, the use of cyber operations to avoid escalation may inadvertently increase its likelihood. By sabotaging adversary military capabilities or degrading command and control structures, subversion promises tactical and operational advantages in case of conflict. Actors have used subversion in such contexts before, for example the Soviet Union in preparation of its invasion of Czechoslovakia in 1968. General Mayorov, the commander of the invading forces, later explained why the Czechoslovakian army failed to anticipate the impending invasion: "The fact is that [former Czechoslovakian] President Ludvik Svoboda stood at the head of the Czechoslovak People's Army as commander-in-chief. And he was our man!"[89] The tactical and operational advantages that a softening up strategy enables in turn promise to lower the expected costs of intervention, thus increasing the perceived relative gains. The greater these expected gains, the likelier actors are to opt for intervention – yet the problem is that cyber operations, like traditional subversion, tend to fall short of delivering on their promise due to their operational constrains. Actors are thus likely to overestimate the gains, while underestimating the costs. The most significant limitation of cyber operations in this context is

[88] Jacquelyn Schneider, 'Cyber and Crisis Escalation: Insights from Wargaming' (U.S. Naval War College, 2017). 12, https://pacs.einaudi.cornell.edu/sites/pacs/files/Schneider.Cyber%20and%20Crisis%20Escalation%20Insights%20from%20Wargaming%20Schneider%20for%20Cornell.10-12-17.pdf.

[89] Miklós Kun, *Prague Spring, Prague Fall: Blank Spots of 1968* (Budapest: Akadémiai Kiadó 1999), 151.

their volatility, marked either by a failure to produce desired effects and a risk of producing unintended effects.[90] Consequently, the expected degradation of adversary capabilities or command and control may fail to manifest in practice, or trigger unexpected reactions. In case of nuclear-armed competitors, the results could be catastrophic.[91] Considering these risks, it is crucial to be aware of the strategic limitations of cyber operations.

Overthrow

The overthrow strategy is likely beyond the reach of cyber operations alone. Electronic communications are useful to establish contact to opposition groups and coordinate their activity from afar. When it comes to providing the material support and training that such groups have often required to be able to mount a successful challenge to an existing government, however, human agents and physical shipments remain necessary.[92] Moreover, taking a more abstract point of view, such local proxy actors exploit vulnerabilities in political systems to undermine and replace a government. This exploitation mechanism exclusively involves human agents and social organizations. As long as computers are not in charge of government (hopefully for a while), cyber operations alone will be incapable of overthrowing governments.

That said, cyber operations can play a possible support role in such operations by attempting to influence public opinion against the existing regime and towards support for the replacement regime. In the Ukrainian case, however, there is considerable evidence that the *failure* of cyber-enabled influence campaigns to sway the Ukrainian population towards Russian interests was a key motivation for Russia's takeover of Crimea as a last resort.[93] In this support role, the same conditions for success as in the strategy of manipulation exist, which cyber manipulation operations have not conclusively shown to fulfil. In short, under current conditions cyber operations are not likely capable of implementing the strategy overthrow, indicating a significant limitation compared to traditional subversion.

Conclusion

The availability of cyber operations does not usher in a new a new epoch of conflict, but offers new tools to implement strategies of subversion. This article first highlighted the parallels between cyber operations and

[90] Maschmeyer, 'The Subversive Trilemma', 64.
[91] Erik Gartzke and Jon R. Lindsay, 'Thermonuclear Cyberwar', *Journal of Cybersecurity* 3/1 (2017), 37–48. doi:10.1093/cybsec/tyw017.
[92] Lee, *Crippling Leviathan*, 145.
[93] Sanshiro Hosaka, 'The Kremlin's "Active Measures" Failed in 2013: That 'S When Russia Remembered Its Last Resort-Crimea', *Demokratizatsiya; Washington* 26/3 (Summer 2018), 321–64.

subversion, a non-military instrument of power marked by its mechanism secret exploitation. Consequently, to advance strategic thought on cyber conflict, it is useful to examine strategies of subversion. I showed that rather than developing new theory on a new phenomenon, as a wave of current scholarship attempts, we can build on theory on an existing phenomenon, subversion, and refine it by examining how information technology changes it. Building on the literature on subversion, I identified three distinct strategies: manipulation, erosion and overthrow. The analysis showed that the greater their potential strategic value is, the greater the operational requirements for success become, and the chance of failure increases accordingly. Hence, subversion provides limited value overall. Evaluating the utility of cyber operations as instruments of each strategy challenged prevailing expectations of their strategic value short of war. Despite current fears of information technology allowing vastly more effective covert operations, it revealed cyber operations to be relatively more constrained in the scope of reach than traditional subversion. This is in line with emerging research showing technological change does not produce a fundamental change in the quality of subversion.[94] Conversely, their presumed superior scale remains unproven. Due to the limits of their reach, overthrow remains beyond the reach of cyber operations alone.

Instead, and contrary to their reputation as high-speed instruments, the analysis revealed cyber operations to be most suited for the slow-burning strategy of erosion. Like the other subversive strategies, it offers states a way to weaken an adversary and gain advantages at lower risks and costs than war. This promise renders subversion highly attractive, and the more destructive war is, the more attractive this alternative becomes. As former United States President John F. Kennedy highlighted in the 1960s,

> the armies are there and in large numbers. The nuclear armaments are there. But they serve primarily as a shield behind which subversion, infiltration, and a host of other tactics steadily advance, picking off vulnerable areas, one by one, in situations which do not permit our own armed intervention.[95]

Today, nuclear armaments remain just as destructive, while conventional armies have become even more lethal. Hence, strategies of subversion are likely even more attractive to leaders.

Yet the erosion strategy face two important limitations. First, it requires significant organizational capacity and resources. Contrary to prevailing expectations of the low barriers to entry in cyber conflict, and resulting asymmetric advantages for weaker actors vis-à-vis stronger actors, these requirements likely reserve the strategy for the largest and most advanced

[94] Maschmeyer, Lennart, ‘Slow Burn: Subversion and Escalation in Cyber Conflict and Covert Action’, doctoral dissertation, University of Toronto, 2020.

[95] Blackstock, *The Strategy of Subversion*, 26.

states. Second, even with these requirements fulfilled, its chance of success is limited due to operational challenges. States are thus likely to continue to use it to try and throw stones in the path of their adversaries. Yet contrary to current expectations, they are unlikely to succeed in producing or preventing measurable shifts in the balance of power.

This strategic theory explains key patterns in cyber conflict. The observation that cyber operations are predominantly used in low intensity competition, independently from warfare, is congruent with expectations. So is the fact that the vast majority of cyber operations focus on espionage rather than active effects.[96] As Mitrokhin's archive shows, the same was the case with Soviet use of illegal agents.[97] Contrary to the predictions of current wisdom, it also explains why, despite the widespread use of cyber operations, there have not been significant shifts in the balance of power as a consequence. Like with traditional subversion, leaders are likely unable to resist its promise despite its practical limitations.

Importantly, this theory indicates is that persistent engagement is not likely a winning defensive strategy. Persistent engagement and the underlying theory correctly identify the type of adversary strategy involved, namely erosion. However, in the ambition to identify one defining, universal characteristic of cyber operations, namely constant contact and the resulting need for persistent engagement,[98] they risk missing other important characteristics that determine effectiveness, i.e., the conditions that need to be met for successful shift in the balance of power short of war. Persistence is important to achieve exploitation. However, so are creativity, skill and stealth. Most importantly, successful subversive operations exploit vulnerabilities to produce effects *before* the victim can detect and mitigate the exploitation. Building a strategy around persistence alone risks underprioritizing these other components. Consequently, it provides opportunities for adversaries to achieve advantages by leveraging the latter. Through creativity and stealth, adversaries can still win against an actor that persistently engages them.[99] Think of someone persistently bashing on the front door of your house, and you sneaking out through the backdoor, stealthily entering your adversaries house to wreak havoc while they are busy.

Instead, building on counterintelligence strategies promises more effective responses in at least three ways. First, rather than a focus on technology reflected in a universal concept of "cyber" as a threat, it underlines the importance of considering the many different types of

[96] See, for example: FireEye, 'M-Trends', 2020. https://content.fireeye.com/m-trends/rpt-m-trends-2020.
[97] Andrew and Mitrokhin, *The Sword and the Shield*.
[98] Fischerkeller and Harknett, 'Cyber Persistence Theory, Intelligence Contests and Strategic Competition'.
[99] Lennart Maschmeyer, 'Persistent Engagement Neglects Secrecy at Its Peril', *Lawfare* (blog), 4 Mar. 2020. https://www.lawfareblog.com/persistent-engagement-neglects-secrecy-its-peril.

(subversive) operations that exploiting information technology enables.[100] Accordingly, rather than a universal solution, strategy should prioritize developing customized counters to these individual types. To be sure, persistent engagement does not preclude doing so – but the focus on a universal framework for a supposedly new threat risks distracting from the historical parallels to subversion and lessons that can be drawn from past operations of different types. Second, it highlights the need to move on from a military mindset of offense and defense to an intelligence mindset of exploitation, deception and detection. In military conflict, when the offense gets through, the defense has failed. In intelligence contests, however, discovery of adversary exploitation offers a counterintelligence opportunity to monitor activity, analyze tradecraft and pre-empt losses. For example, counterintelligence techniques to lay traps for opponents to discover them and identify their sponsors promises key benefits. Rather than engagement, in many cases it is likely beneficial to monitor activity, dissect tools and techniques to neutralize them and possibly guide the activity where it can produce the least harm. It also offers an opportunity to compromise adversary infrastructure to gather further intelligence. Similarly, the importance of distrust in counterintelligence to limit vulnerabilities and identify intruders can be directly applied to the problem of cybersecurity.[101] Finally, building on proven counterintelligence techniques also promises greater effectiveness against a likely future development: operations and campaign that combine both traditional and cyber instruments of subversion to offset their relative shortcomings and maximize the scope and scale of reach. Such integrated means could conceivably expand the strategic value of subversion, yet will be highly complex to coordinate and implement.

Acknowledgments

The author would like to thank Max Smeets and the anonymous reviewers for constructive feedback on earlier drafts of this article.

Disclosure statement

No potential conflict of interest was reported by the author(s).

[100] For an overview of the vast range of covert operations there are, see, for example: Johnson, 'On Drawing a Bright Line for Covert Operations'.

[101] Loch K. Johnson (ed.), *Strategic Intelligence, Volume 4: Strategic Intelligence: Counterintelligence and Counterterrorism*, Vol. 4, Intelligence and the Quest for Security (Westport, Conn: Praeger Security International 2007), 9–11.

Notes on contributor

Lennart Maschmeyer is a Senior Researcher at the Center for Security Studies at ETH Zurich. He holds a PhD in Political Science from the University of Toronto and an MPhil in International Relations from the University of Oxford. Lennart's research examines the nature of cyber power, operational mechanisms of cyber conflict and resulting strategic dynamics as well as knowledge production processes in cybersecurity. He is the founder co-chair of the FIRST Threat Intel Coalition SIG, an initiative to assist vulnerable civil society organizations in preventing, detecting and mitigating cyber attacks. He is also the founder and co-chair of the European Cybersecurity Seminar, which brings together academics and practitioners in cybersecurity and provides them a platform to present research projects and receive feedback.

References

Andrew, Christopher M. and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*, 1st ed. (New York: Basic Books 1999).

Andrew, Christopher M., *The Mitrokhin Archive: The KGB in Europe and the West* (London: Allen Lane 2000).

Arquilla, John and David Ronfeldt. 'Cyberwar is Coming!', *Comparative Strategy* 12/2 (1 Apr. 1993), 141–65. doi:10.1080/01495939308402915.

Bail, Christopher A., Brian Guay, Emily Maloney, Aidan D. Combs, Sunshine Hillygus, Friedolin Merhout, Deen Freelon, and Alexander Volfovsky, 'Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017', *Proceedings of the National Academy of Sciences* 117/1 (7 Jan. 2020), 243–50. doi:10.1073/pnas.1906420116.

Barron, John, *KGB: The Secret Work of Soviet Secret Agents* (London: Hodder and Stoughton 1975).

Beilenson, Lawrence W., *Power Through Subversion* (Washington DC: Public Affairs Press 1972.

Bittman, Ladislav, *The KGB and Soviet Disinformation: An Insider's View* (Washington DC: Pergamon-Brassey's 1985).

Blackstock, Paul W., *The Strategy of Subversion: Manipulating the Politics of Other Nations* (Chicago: Quadrangle Books 1964).

Brantly, Aaron Franklin, *The Decision to Attack: Military and Intelligence Cyber Decision-Making*, (Athens, GA: University of Georgia Press 2016. http://muse.jhu.edu/book/45365.

Brantly, Aaron F., N. Cal, and D. Winkelstein, 'Defending the Borderland', Report: Army Cyber Institute, 1 Dec. 2017. https://vtechworks.lib.vt.edu/handle/10919/81979.

Buchanan, Ben, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard UP 2020).

Callanan, James, Covert Action in the Cold War: US Policy, Intelligence and CIA Operations (New York: I.B.Tauris 2009).

Carson, Austin, *Secret Wars: Covert Conflict in International Politics* (Princeton, NJ: Princeton UP, 2018).

Denison, Benjamin C., *Strategies of Domination: Uncertainty, Local Institutions, and the Politics of Foreign Rule* (University of Notre Dame 2018). https://curate.nd.edu/show/j6731260871.

DoD, 'Strategy for Operating in Cyberspace', 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Downes, Alexander B., *Catastrophic Success: Why Foreign-Imposed Regime Change Goes Wrong* (Ithaca, New York: Cornell UP 2021).

Dullien, Thomas, 'Weird Machines, Exploitability, and Provable Unexploitability', *IEEE Transactions on Emerging Topics in Computing* 8/2 (Apr 2020), 391–403. doi:10.1109/TETC.2017.2785299.

Dunn Cavelty, Myriam, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', *International Studies Review* 15/1 (2013), 105–22. doi:10.1111/misr.12023.

Erickson, Jon, *Hacking: The Art of Exploitation* (San Francisco: No Starch Press 2003).

Erik, Gartzke and Jon R. Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', *Security Studies* 24/2 (3 Apr. 2015): 316–48. doi:10.1080/09636412.2015.1038188.

ESET, 'BlackEnergy Trojan Strikes Again: Attacks Ukrainian Electric Power Industry', *WeLiveSecurity* (blog), 4 Jan. 2016. https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/.

ESET, 'Bad Rabbit: Not-Petya is Back with Improved Ransomware', *WeLiveSecurity (blog)*, 24 Oct. 2017. https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/.

FireEye, 'M-Trends', 2020. https://content.fireeye.com/m-trends/rpt-m-trends-2020.

Fischerkeller, Michael P. and Richard J. Harknett, 'Deterrence is Not a Credible Strategy for Cyberspace', *Orbis* 61/3 (1 Jan. 2017), 381–93. doi:10.1016/j.orbis.2017.05.003.

Fischerkeller, Michael P. and Richard J. Harknett, Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation', *The Cyber Defense Review* (2019), 267–87. doi:10.2307/26846132.

Fischerkeller, Michael, *The Structural and Strategic Imperative: The Need for Persistent Engagement* (IDA n.d.). https://www.ida.org/research-and-publications/-/media/2e11bf09b5a44cb49e59571704171218.ashx.

Gartzke, Erik, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security* 38/2 (2013), 41–73. doi:10.1162/ISEC_a_00136.

Gartzke, Erik and Jon R. Lindsay, 'Thermonuclear Cyberwar', *Journal of Cybersecurity* 3/1 (2017), 37–48. doi:10.1093/cybsec/tyw017.

Goodman, Will, 'Cyber Deterrence: Tougher in Theory Than in Practice?', *Strategic Studies Quarterly* 4/3 (Fall 2010), 102–35.

Gorwa, Robert and Max Smeets, 'Cyber Conflict in Political Science: A Review of Methods and Literature', Preprint. SocArXiv, 25 July 2019. doi:10.31235/osf.io/fc6sg.

Greenberg, Andy, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, 22 Aug. 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Grey, Stephen, *The New Spymasters: Inside the Modern World of Espionage from the Cold War to Global Terror* (New York: St. Martin's Press 2015).

Harknett, Richard J. and Max Smeets, 'Cyber Campaigns and Strategic Outcomes', *Journal of Strategic Studies* (4 Mar. 2020), 1–34. doi:10.1080/01402390.2020.1732354.

Healey, Jason and Karl Grindal (eds.), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association 2013).

Hosaka, Sanshiro, 'The Kremlin's 'Active Measures' Failed in 2013: That 's When Russia Remembered Its Last Resort-Crimea', *Demokratizatsiya; Washington* 26/3 (Summer 2018), 321–64.

Jamieson, Kathleen Hall, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President What We Don't, Can't, and Do Know* (New York, NY: Oxford UP 2018).

Johnson, Loch K., 'On Drawing a Bright Line for Covert Operations', *The American Journal of International Law* 86/2 (1992), 284–309. doi:10.2307/2203235.

Johnson, Loch K. (ed.) *Strategic Intelligence, Volume 4: Strategic Intelligence: Counterintelligence and Counterterrorism*. Vol. 4. (Westport, Conn: Praeger Security International 2007).

Johnson, Loch K., *The Third Option: Covert Action and American Foreign Policy* (Oxford: Oxford UP 2022).

Kello, Lucas, *The Virtual Weapon and International Order* (Yale: Yale UP 2017).

Kitson, Frank, *Low Intensity Operations: Subversion, Insurgency, Peacekeeping*. (London: Faber 1971).

Kostyuk, Nadiya and Yuri Zhukov, 'Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?', *The Journal of Conflict Resolution* 63/2 (2017), 317–47. doi:10.1177/0022002717737138.

Kugler, Richard L., 'Deterrence of Cyber Attacks', in Kramer, Franklin D., Starr, Stuart H. & Wentz, Larry K. (eds.), *From Cyberspace to Cyberpower: Defining the Problem* (Washington DC: Potomac Books 2009), 309–42.

Kun, Miklós, *Prague Spring, Prague Fall: Blank Spots of 1968* (Budapest: Akadémiai Kiadó 1999).

Langner, Ralph, 'To Kill a Centrifuge', Nov. 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Leber, Andrew and Alexei Abrahams, 'A Storm of Tweets: Social Media Manipulation During the Gulf Crisis', *Review of Middle East Studies* 53/2 (Dec. 2019), 241–58. doi:10.1017/rms.2019.45.

Lee, Melissa M., *Crippling Leviathan: How Foreign Subversion Weakens the State*. (Ithaca, New York: Cornell UP 2020).

Levin, Dov H., *Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions* (New York: Oxford UP 2020).

Libicki, Martin C., *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND 2009).

Lindsay, Jon R., 'Stuxnet and the Limits of Cyber Warfare', *Security Studies* 22/3 (2013), 365–404. doi:10.1080/09636412.2013.816122.

Lindsay, Jon R., 'Restrained by Design: The Political Economy of Cybersecurity', *Digital Policy, Regulation and Governance* 19/6 (26 July 2017), 493–514. doi:10.1108/DPRG-05-2017-0023.

Lindsay, Jon R. and Erik Gartzke, 'Coercion Through Cyberspace: The Stability-Instability Paradox Revisited', in Peter Krause (ed.), *The Power to Hurt: Coercion in Theory and in Practice* (New York: Oxford UP 2018), 179–203.

Lynn, William J., III, 'Defending a New Domain', *Foreign Affairs* (2010). https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

Maschmeyer, Lennart, 'Slow Burn: Subversion and Escalation in Cyber Conflict and Covert Action', doctoral dissertation, University of Toronto, 2020.

Maschmeyer, Lennart, 'Persistent Engagement Neglects Secrecy at Its Peril', *Lawfare* (blog), 4 Mar. 2020. https://www.lawfareblog.com/persistent-engagement-neglects-secrecy-its-peril.

Maschmeyer, Lennart, 'Digital Disinformation: Evidence from Ukraine', CSS Analysis No. 278, Feb. 2021. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse278-EN.pdf.

Maschmeyer, Lennart, 'The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations', *International Security* 46/2 (Oct. 2021), 51–90. doi:10.1162/isec_a_00418.

Maschmeyer, Lennart and Nadiya Kostyuk, 'There is No Cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict', *War on the Rocks* (blog), 8 Feb. 2022. https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/.

McGraw, Gary, 'Cyber War is Inevitable (Unless We Build Security In)', *Journal of Strategic Studies* 36/1 (Feb. 2013), 109–19. doi:10.1080/01402390.2012.742013.

Michael, Fischerkeller and Richard J. Harknett, 'Cyber Persistence Theory, Intelligence Contests and Strategic Competition', Institute for Defense Analysis, June 2020. https://apps.dtic.mil/sti/pdfs/AD1118679.pdf.

Michels, Eckard, *Guillaume, Der Spion: Eine Deutsch-Deutsche Karriere* (Berlin: Ch. Links Verlag 2013).

Nakasone, Paul M. and Michael Sulmeyer, 'How to Compete in Cyberspace', 17 Mar. 2021. https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

Nye, Joseph S., 'Nuclear Lessons for Cyber Security?', *Strategic Studies Quarterly* 5/4 (Winter 2011), 18–38.

O'-Rourke, Lindsey A., *Covert Regime Change: America's Secret Cold War*. (Ithaca, NY: Cornell UP 2018).

OSS, 'Simple Sabotage Field Manual', 1944.

Rid, Thomas, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35/1 (Feb. 2012), 5–32. doi:10.1080/01402390.2011.608939.

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

Rovner, Joshua and Tyler Moore, 'Does the Internet Need a Hegemon?', *Journal of Global Security Studies* 2/3 (1 July 2017), 184–203. doi:10.1093/jogss/ogx008.

Rovner, Joshua, Cyber War as an Intelligence Contest, *War on the Rocks*, 16 Sept. 2019. https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

Ruck, Damian J., Natalie M. Rice, Joshua Borycz, and R. Alexander Bentley, 'Internet Research Agency Twitter Activity Predicted 2016 U.S. Election Polls', *First Monday* 24/7 (30 June 2019). doi:10.5210/fm.v24i7.10107.

Schneider, Jacquelyn, *Cyber and Crisis Escalation: Insights from Wargaming* (U.S. Naval War College 12 2017). https://pacs.einaudi.cornell.edu/sites/pacs/files/Schneider.Cyber%20and%20Crisis%20Escalation%20Insights%20from%20Wargaming%20Schneider%20for%20Cornell.10-12-17.pdf.

Shultz, Richard H. and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy* (Washington DC: Pergamon-Brassey's 1984).

Slayton, Rebecca, 'What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment', *International Security* 41/3 (Jan. 2017), 72–109. doi:10.1162/ISEC_a_00267.

Smeets, Max, 'The Strategic Promise of Offensive Cyber Operations', *Strategic Studies Quarterly* 12/3 (Fall 2018).

Specops, 'The Countries Experiencing the Most 'Significant' Cyber-Attacks' Specops Software',9 July 2020. https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/.

Stone, John, 'Cyber War Will Take Place!', *Journal of Strategic Studies* 36/1 (2013), 101–08. doi:10.1080/01402390.2012.730485.

US CYBERCOM, 'Achieve and Maintain Cyberspace Superiority - Command Vision for US Cyber Command', Apr. 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

US Treasury, Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks | U.S. Department of the Treasury', 15 Mar. 2018. https://home.treasury.gov/news/press-releases/sm0312.

Waldman, Arielle, ‘FBI: Ransomware Hit 649 Critical Infrastructure Entities in 2021’, *Search Security*, 24 Mar. 2022. https://www.techtarget.com/searchsecurity/news/252515076/FBI-Ransomware-hit-649-critical-infrastructure-entities-in-2021.

The White House, ‘International Strategy for Cyberspace’, 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Williams, Brad D., ‘Nakasone: Cold War-Style Deterrence ″does Not Comport to Cyberspace″’, *Breaking Defense* (blog), 4 Nov. 2021. https://breakingdefense.sites.breakingmedia.com/2021/11/nakasone-cold-war-style-deterrence-does-not-comport-to-cyberspace/.

Wirtz, James J., ‘The Cyber Pearl Harbor’, in Goldman, Emily O. and Arquilla, John (eds.), *Cyber Analogies* (Monterey, CA: Naval Postgraduate School 2014), 7–14.

Wohlforth, William C., ‘Realism and Great Power Subversion’, *International Relations* 34/4 (1 Dec. 2020), 459–81. doi:10.1177/0047117820968858.