The Cyber Character of Political Warfare

Benjamin Jensen

The world is witnessing the reawakening of an old strategic practice: political warfare. The connectivity of the modern world puts a premium on coercive diplomacy in the shadows. States such as Russia conduct a “new form of political sabotage,” using a mix of cyberpower and propaganda to attack electoral institutions and undermine faith in the democratic process. Moscow uses cyber operations to carry out covert, coercive campaigns short of war; it tampered with elections and disseminated fake news across multimedia in Ukraine in 2014, the United States in 2016, and France in 2017.

Cyber incidents such as these show how states are mixing the old with the new. Much like the early Cold War, emerging cyber operations combine espionage, propaganda, economic warfare, and sabotage in an effort to signal resolve and shape adversaries’ foreign policies. The character of war and strategic competition is changing. The new cold war is online, yet just as fraught with escalation risks and uncertainty as it was 30 years ago.

This article draws on early Cold War declassified documents and historiography as well as the emerging literature on cyber operations to explore the changing character of strategic competition and coercion. While the “Third Offset”—with its promise of a military affairs revolution defined by unmanned battlefields and artificial intelligence—grabs the headlines, a more subtle change is taking place beneath the surface. States are discovering how to use cyber coercion as a means of undermining adversaries and influencing those adversaries’ foreign policy options. This article proceeds by defining political warfare, drawing out examples of key operational forms, and situating them within the
larger academic literature on coercion and coercive diplomacy. From this vantage point, the article reviews the literature on cyber coercion and demonstrates how hacking becomes a form of political warfare in the twenty-first century. Specifically, examples of psychological warfare and sabotage through cyber operations demonstrate the utility—and limits—of online political warfare.

**Defining Political War**

In a classified 1948 Policy and Planning Staff Memorandum, George Kennan defined political warfare as operations that “range from such covert actions as political alliances, economic measures, and white propaganda to such covert operations as clandestine support to friendly foreign elements, black psychological warfare and even encouragement of underground resistance in hostile states.”

Whereas “white propaganda” reveals its origin, “black psychological warfare” hides its origin and can denote false statements attributed to other groups in order to undermine them.

For Kennan, political warfare was “the logical application of Clausewitz’s doctrine in time of peace. In broadest definition, political warfare [was] the employment of all means at a nation’s command, short of war, to achieve its national objectives.”

Political warfare is, from a theoretical perspective, an example of coercion.

In international relations, coercion is the use of threats and limited action to alter behavior. It is more potential than actual force; it takes minimal, often indirect action to alter the cost-benefit calculation of an adversary short of using such brute force as would result in a major military campaign. Avoiding brute force is the key to coercion: force is threatened, or even used at a lower threshold short of open battle, to achieve a concession short of war. Hence, for Nobel Laureate Thomas Schelling, coercion is the exploitation of potential force.

Given its clandestine nature and indirect approach, political warfare works in the background to increase the credibility of other threats and to undermine the adversary’s ability to resist. The central task of any coercive strategy is “to create in the opponent the expectation of costs of sufficient magnitude to erode his motivation to continue what he is doing.” In this, success depends “on whether the initial coercive action or threat stands alone or is part of a broader credible threat to escalate pressure further if necessary.” Political warfare shapes the environment, animating this “broader credible threat” by creating risk and
uncertainty for the target. It is not a clear signal, but rather a wave of background noise that limits the target’s freedom of action. That is, the task is more about increasing the cost of making choices that are unfavorable to the initiator than it is about forcing a concession.  

Political warfare was a key vector of competition during the Cold War. Before the missile gap, there was an influence gap. And, for many leading thinkers of the time, the Soviets were masters of political warfare. According to Kennan, “Lenin so synthesized the teachings of Marx and Clausewitz that the Kremlin’s conduct of political warfare has become the most refined and effective of any in history.” A declassified 1951 CIA memorandum echoed this perspective, asserting that “in the Soviet concept, a state of political and psychological warfare is the normal relationship between Communist and capitalist states. Armed conflict is merely the employment of additional means in the conduct of this continuing struggle.” Officials also assumed that political warfare would be a key component of any larger military attack by the Soviet Union. According to a 9 May 1950 CIA memorandum, “The USSR regards political and psychological warfare as integral rather than incidental in the waging of war.” Political warfare was a means of coercing an adversary before hostilities and, once the fighting began, a means of undermining its cohesion.

To respond to such coercion, the United States needed its own means to undermine the Soviets from within while pursuing a strategy of containment. Contrary to the view of containment as a defensive posture, thinkers such as Kennan “advocated an aggressive program of clandestine warfare against Communism, involving propaganda, sabotage, subversion, and paramilitary engagement.” Visions of early political warfare efforts included low-cost, low-risk, plausibly deniable methods for undermining Soviet resolve and cohesion while limiting communist expansion.

These activities built on Allied efforts in World War II. In 1939, British Colonel Lawrence Grand, head of the War Office GS(R), circulated a paper advocating for an irregular warfare approach to challenging the Axis powers. Hugh Dalton, the British Minister of Economic Warfare, picked up these ideas and helped lay the groundwork for the Special Operations Executive (SOE). Dalton served as a member of the executive committee of the Political Warfare Executive. The organization helped create an infrastructure for resistance in neutral and Axis-occupied countries through activities ranging from setting up wireless communication to building networks of resistance groups.

On the other side of the Atlantic, the U.S. Office of Strategic Services also ventured into the world of political warfare. According to unclassified doctrinal
manuals, “strategic services” were “all measures taken to enforce our will upon
the enemy by means other than military action.” These actions included ac-
tivities designed “to aid and give direct support to the furtherance of protected
or actual military operations; to destroy the will and ability of the enemy to
resist; and to deprive the enemy of the support of his allies and of neutrals and
strengthen resistance within occupied countries.”

For example, the political warfare plan for Operation Overlord—the 1944
Normandy invasion—called for undermining German morale through various
activities, including appealing to over six million foreign workers in Germany
to slow down production and supporting resistance movements in the Balkans
as a means of tying down German military units. The plan stated that politi-
cal warfare “must, at the proper time, exploit and canalize political ferments
existing behind enemy lines” in support of larger objectives, including bombing
campaigns, deception operations, and major ground campaigns.

As such, the concept of political warfare and strategic services was a logi-
cal referent for strategists seeking to counter the Soviet Union in 1947. In
December of that year, the Truman administration published NSC 4-A, which
tasked the CIA with taking the lead on covert psychological warfare operations
that reflected elements of earlier efforts in World War II. The declassified direc-
tive opened by stating:

the National Security Council, taking cognizance of the vicious
psychological efforts of the USSR, its satellite countries, and
Communist groups to discredit and defeat the aims and activities of
the United States and other Western powers, has determined that, in
the interests of world peace and U.S. national security, the foreign
information activities of the U.S. Government must be supplemented
by covert psychological operations.

By the summer of 1948, the renewed focus on psychological warfare
broadened to include covert action operations when the Truman administration
published NSC 10/2. The document advocated political warfare and called for
a new organization, the Office of Policy Coordination (OPC), to coordinate
propaganda; economic warfare; preventive direct action, including sabotage,
anti-sabotage, demolition, and evacuation measures; subversion against hostile
states, including assistance to underground resistance movements, guerrillas, and
refugee liberation groups; and support of indigenous anti-communist elements
in threatened countries of the free world.

The table below lists the new organization’s lines of effort, referred to in
the document as lines of clandestine activity, based on an October 1948 declas-
One of the predominant forms of political warfare in the early Cold War was psychological warfare. Poison pens—false letters sent to undermine an enemy—and rumors were techniques used by the Office of Strategic Services (OSS) during World War II and subsequently adopted by the new OPC. During Operation Hemlock in World War II, anonymous letters containing rumors that officials engaged in activity in support of the Allies were sent to Gestapo officers. In a
separate operation, OSS operatives created a fake holiday greeting from a German mayor and sent it to frontline troops. The letter outlined sacrifices on the home front designed to undermine German military confidence in the Nazi regime.\textsuperscript{30}

False flags—making it seem as if an act was carried out under another nation’s flag—were a form of covert action designed to manipulate perception and undermine morale and cohesion. A group attempts to conceal its involvement by creating the perception that a separate group made an inflammatory statement and carried out some act of sabotage, subversion, or physical attack. For example, during the September 1931 Mukden incident, Japan covertly blew up a section of railway in Manchuria and shifted the blame onto China as a pretext for seizing the territory and installing a puppet government.\textsuperscript{31}

Much of the earlier psychological warfare efforts focused not only on these rumors and false flags, but also on building an infrastructure for disseminating ideas that countered Soviet propaganda. For example, the CIA covertly established Radio Free Europe/Radio Liberty under the veil of a private broadcaster to “contribute to the liberation of the nations imprisoned by the Iron Curtain by sustaining their morale and stimulating in them a spirit of non-cooperation with Soviet-dominated regimes.”\textsuperscript{32}

\textbf{Figure 2: How to Undermine a State from Within (1950)}\textsuperscript{35}

The agency also established state-private networks that used private groups—ranging from foundations and action committees to arts organizations—to undermine Soviet messaging and shape the occupied areas for liberation.\textsuperscript{33} These included the Crusade for Freedom fundraising drives, which sponsored exile programming on Radio Free Europe/Radio Liberty.\textsuperscript{34}
**The Cyber Character of Political Warfare**

*SABOTAGE*

Another key attribute of political warfare was sabotage and preventive action that undermined an adversary’s critical capabilities and cohesion short of armed conflict. As seen in Figure 1, this logic extended beyond the CIA to the military services. By 1950, the U.S. Army published a series of classified manuals to support unconventional military activity in support of political warfare. As the figure illustrates, indirect action could limit the connection between political leaders and the economic sector, as well as between the economic sector and security services.

**Political Warfare Comes of Age in Cyberspace**

Cyber operations offer a new vector of covert political warfare. Cyber coercion involves digitally exploiting “the power to hurt.” Intrusions, logic bombs, website defacements, viruses, and distributed denial-of-service (DDoS) operations indirectly compel an adversary without physical attack. Through these measures, an actor’s power to hurt becomes “the power to hurt online.” Martin Libicki situates cyber operations on an escalation ladder between economic coercion and the use of physical force short of nuclear exchange.

In peacetime competition, cyber coercion is an indirect and additive form of compellence. Compellence refers to using coercive action to change a state’s existing behavior. The concept can be differentiated from deterrence, which seeks to stop a state from taking aggressive action. Cyber coercion is indirect because it signals in the covert sphere—like early forms of political warfare—and achieves success by enhancing perceptions of resolve and managing escalation, rather than by employing direct, overt threats. Even when cyber operations fail to achieve a concession, they signal the risk of escalation and demonstrate resolve. Cyber coercion is additive in that, like coercive diplomacy, success depends “on whether the initial coercive action or threat stands alone or is part of a broader credible threat to escalate pressure further if necessary.” The extension of classical political warfare operations such as psychological warfare and sabotage to the digital domain demonstrates this logic.

**Psychological Warfare: Weaponizing Fake News**

The hacking of the 2016 U.S. election demonstrated how countries combine cyber espionage with traditional psychological warfare techniques in the twenty-
first century. First, Russian-linked groups penetrated the Democratic National Committee and other political networks using spearphishing methods to steal private correspondence. Once they stole the data, they could selectively determine what to release, even adding their own propaganda twists, at key intervals to disrupt the election and demonstrate the purported weakness of American political institutions. Furthermore, building on the Soviet tradition of active measures—covert psychological warfare efforts designed to undermine a rival population’s morale or faith in their political leaders—Russian operatives used botnets to disseminate fake news targeting key demographics. The result was a sustained barrage of news circulated on social media designed to undermine the election.

Russia also routinely uses false flags to enable poison pens and rumors in Ukraine. These activities are indirect and coercive; they both signal resolve and isolate the target. For instance, CyberBerkut, a hacking coalition named after the Ukrainian interior police forces, had clear connections to Moscow. In March 2015, the group claimed to have hacked into U.S. defense contractors and Ukrainian government servers, stealing documents that showed plans to move U.S. weapons into Ukraine. To undermine international perceptions of the Ukrainian government, CyberBerkut also released “hacked” documents claiming to show that the Ukrainian military supplied weapons to the Islamic State. The group also sought to implicate nonprofits that support civil society development, releasing documents—allegedly hacked from the Soros Foundation—showing that George Soros was pressuring U.S. officials to provide lethal assistance to Ukraine. In June 2017, the United Arab Emirates triggered a diplomatic crisis in the Persian Gulf by taking control of a Qatari website. After hacking the online news feed, the group planted false information showing the Emir praising Iran and calling for good relations with Israel while contradictorily supporting Hamas and the Muslim Brotherhood. The intrusion was followed by a massive DDoS attack on Al Jazeera, the Qatari-owned media outlet. In effect, cyber operatives conducted a classic psychological warfare operation that undermined the integrity of an alliance network. News agencies in multiple Gulf States ran with the false story, leading to a diplomatic and economic blockade of Qatar by Saudi Arabia, Bahrain, Egypt, Jordan, and the United Arab Emirates.

**Sabotage with a Cyber Twist**

Cyber coercion provides a new vector for sabotage as part of larger coercive
diplomatic efforts. These efforts tend only to succeed when combined with broader threats and positive inducements, as was the case in the famed Stuxnet attack on Iranian nuclear facilities.

Stuxnet began more as a means of delaying military action during complex negotiations than a plan to decisively cripple Iranian enrichment. In this respect, the operation was more an example of covert action and sabotage than of a conventional precision strike. Such operations rely on significant intelligence preparation to find a critical vulnerability.

Operators in the United States began working on the Stuxnet worm as early as 2005. Development likely accelerated after Israel requested U.S. assistance for limited military strikes against Iranian nuclear facilities in Natanz. In 2009, developers modified Stuxnet by shifting the attack vector from targeting valve pressure to stress centrifuge rotation frequency in an effort to increase the worm’s destructive potential. Between 2009 and 2010, this modified approach led to a 23 percent decline in the number of operational centrifuges.

Yet, the initial destructive effect of the cyber sabotage campaign was limited and temporary. Stuxnet was not a low-cost, high-payoff offensive success by itself. Subsequent studies suggested the degradation effort was much more costly in terms of time, people, and resources than originally estimated. Rebecca Slayton’s case study highlights that Stuxnet likely cost US$300 million and produced a situation in which the offensive cost more than the defense. In comparison, the cost of a Tomahawk land attack cruise missile is US$1.59 million. For example, the 59 missiles launched at the Syrian air base in April 2017 cost—excluding sunk costs for ships and development—approximately US$93 million. For the cost of Stuxnet, and with no guarantee of success, the United States or Israel could have launched three cruise missile offensive strikes. Furthermore, these strikes would have had higher confidence and easier battle damage assessments. Lastly, Stuxnet burned important zero-day exploits and stolen certificates, and revealed intelligence methods that could have been used in future coercive cyber campaigns. Stuxnet demonstrated the difficulty leaders face weighing costs and benefits with respect to covert action. Leaders trade the ability to further penetrate a network—collecting intelligence and preparing for a future strike—for a short-term, often uncertain coercive effect. They trade the assured destruction of a military strike for the limited escalation risk of a cyber intrusion.

What tipped Iranian leaders away from pursuing nuclear capabilities (at least in the short-term) was the larger, multilateral coercive diplomatic effort involving diplomatic isolation, economic sanctions, and the threat of military
action. Stuxnet was one piece of the puzzle, signaling resolve and the risks associated with a continued standoff. This finding demonstrates the unique character of cyber coercion, and with it modern political warfare: the effects tend to be indirect and additive. That is, coercion occurs through a carrot-and-stick approach, combining positive and negative inducements. Covert action, in the case of the Stuxnet cyber sabotage, supports this campaign by indirectly signaling resolve and the risks of escalating the crisis.

Conclusion

Cyber coercive campaigns are online political warfare. They work in an indirect and additive manner to coerce rivals and signal resolve. In this reading, Russian election hacks are simply contemporary examples of classical political warfare campaigns akin to CIA efforts to manipulate the 1948 Italian election. Through psychological operations that spread false accounts and play on media bias, cyber operations can manipulate information and have the potential to change electoral outcomes. Similarly, high-profile cyber intrusions like Stuxnet reflect sabotage in a digital age.

The future is more likely to involve dueling psychological warfare campaigns and covert action designed to undermine adversaries than open conflict between great powers. New cold wars will entail a series of cyber disputes and propaganda campaigns that allow states to manage escalation while seeking a position of advantage. There will be a new stability-instability paradox. While the risk of great power conflict will remain low, there will likely be a proliferation in low-level cyber intrusions that risk increasing the means available for cyber operations by criminals and other cyber actors. Unlike a saboteur’s explosive charge, high-end cyber-sabotage vehicles like Stuxnet do not disappear on impact. They proliferate and live on as new tools for cybercriminals to exploit and other state and non-state actors to replicate. Cyber political warfare proliferates in a way that classical political warfare does not.

Like classical political warfare, cyber coercion also carries with it a small, but important, risk of inadvertent escalation. Like the early Cold War, rival states will need to determine new red lines regarding how far covert action can go before it risks triggering overt warfare. For Schelling, “The mixture of conflict and mutual dependence that epitomizes bargaining situations” puts a premium on communicating intentions—either directly or tacitly—through action, and gaining intelligence about the other side’s next move. In these bargaining situations, “The best choice for either [actor] depends on what he expects the other
to do, knowing that the other is similarly guided, so that each is aware that each must try to guess what the second guesses the first will guess the second to guess and so on, in the familiar spiral of reciprocal expectations.”

Guess wrong, and you escalate, creating a dangerous conflict spiral. This dynamic implies that policymakers should approach cyber operations and contemporary political warfare with restraint. Keeping strategic competition confined to covert realms gives leaders flexibility and prevents dangerous military conflicts.

**Notes**

6. Ibid.
8. Ibid.
12. Ibid.
16. Ibid.
Benjamin M. Jensen


22. Ibid.


24. Ibid.


26. Memorandum from the Executive Secretary of the National Security Council (Souers) to Director of Central Intelligence Hillenkoetter, 1947, Emergence of the Intelligence Establishment, document 257, https://history.state.gov/historicaldocuments/frus1945-50Intel.


36. Schelling, Arms and Influence, 2.


41. For examples of how covert action between rivals can produce sunk costs and counter-escalation risks, see: Carson and Yarhi-Milo, “The Intelligibility and Credibility of Signaling.”
50. Ibid.
52. Ibid., 94.
60. Ibid.
Copyright of Brown Journal of World Affairs is the property of Brown University and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.