CENTER FOR LONG-TERM CYBERSECURITY

CLTC OCCASIONAL WHITE PAPER SERIES

Cyber Operations in Conflict

LESSONS FROM ANALYTIC WARGAMES

BENJAMIN JENSEN AND DAVID BANKS

CLTC OCCASIONAL WHITE PAPER SERIES

Cyber Operations in Conflict

LESSONS FROM ANALYTIC WARGAMES

BENJAMIN JENSEN AND DAVID BANKS

CENTER FOR LONG-TERM CYBERSECURITY

Contents

Executive Summary

Headlines about cyber warfare often focus on doomsday scenarios, with depictions of nation-states using "cyber bombs" to remotely dismantle electric grids and other critical infrastructure. Yet recent events—including Russia's use of cyber operations for information warfare and propaganda—suggest that policymakers and military leaders need to broaden their assumptions about how state and non-state actors are likely to use such operations in future crises and conflicts.

To investigate the role of cyber operations in diverse crisis scenarios, we developed two distinct *wargames*—an innovative methodology for investigating competition among diverse actors—to determine likely strategic preferences. In the *Island Impact* game, players represented either the U.S. or China in a simulated crisis in the South China Sea. In *Netwar*, players took on the role of either a national government or one of three opposition groups (a violent non-state actor, major international firm, or cyber activist network) in the context of an escalating conflict. We first ran these games with university students and national security professionals to examine how the participants approached incorporating cyber capabilities with more conventional tools of statecraft. We then constructed a survey experiment involving more than 3,000 internet users to identify which of the strategies identified in the wargame they preferred.

The wargames and survey experiments both showed that cyber capabilities instead produce a *moderating* influence on coercive exchanges and crisis escalation. Cyber-based instruments of power appear to offer states a means of managing escalation 'in the shadows'. Cyber conflict appears in these simulations to resemble covert action and looks more like the 'political warfare' of the Cold War than it does a military revolution. Our work suggests that leaders should think about cyber exchanges in crisis settings more as political warfare and subterfuge than as traditional warfighting.

Among our other key findings:

- **Cyber exchanges will not necessarily be escalatory:** Particularly in state-to-state crises, participants were restrained in their use of cyber tools, suggesting that cyber capabilities may not necessarily be a preferred choice for provocative escalations.

- **Cyber deterrence may be overhyped:** In the context of cyberspace, the logic of coercion—the use of threats and limited action to alter behavior[1]—is less about deterrence (i.e. the threat of force) than about signaling resolve and undermining adversaries from within.

- **Power disparities had limited influence on decision-making:** Even players who were more powerful than their opponents used restraint, suggesting that cyber operations may in fact help stabilize strategic interactions between rivals.

- **Regime type informs cyber strategy preferences:** Actors took a more defensive posture when the polity they were contesting was a democracy, as opposed to an autocracy.

- **Cyber strategy is "issue-agnostic":** The nature of the conflict has little impact on the use of cyber capabilities, as different issues driving conflict—i.e., ideology or ethnic minority rights—did not produce observable differences in cyber strategy preferences.

This report, sponsored by the UC Berkeley Center for Long-Term Cybersecurity, further details our research and findings, and provides an overview of the implications for policymakers and military leaders as they make decisions about cybersecurity and anticipate how rivals will use cyberspace in future crises.

Background

The connectivity of the modern world places a premium on conducting coercive diplomacy in the shadows. States like Russia have demonstrated what the *New York Times* has called a "new form of political sabotage," combining cyber power and propaganda to attack electoral institutions and undermine faith in the democratic process.[2] Through election tampering and fake news disseminated across multimedia in Ukraine, the United States, and France, Moscow demonstrated how cyber operations can enable covert coercive campaigns that have a significant impact, but fall short of war.[3] Other nations have also used cyber operations for coercive purposes, including creating rifts among autocratic allies (see sidebar below).

State actors are not alone in employing digital resources to coerce adversaries. Non-state actors like Daesh/the Islamic State have launched website defacements and used social media sites to conduct activities ranging from recruitment to collecting information on military personnel for retaliatory strikes against their families. In Spring 2015, Daesh hacked Facebook accounts and released the names of 100 military families in an effort to inspire lone-wolf attacks inside the United States.[4] Non-state groups have also challenged each other in the digital domain, in some cases creating multi-party rivalries, such as disputes between Anonymous and Daesh,[5] and Anonymous and the Zetas Drug Cartel in Mexico.[6] Meanwhile, a growing number of governments today employ online tools to control their populations.[7]

The Case of Qatar: Cyber as Coercive Instrument

In June 2017, the United Arab Emirates reportedly triggered a diplomatic crisis in the Persian Gulf by taking control of a Qatari website. After hacking the website's online news feed, the group planted false information showing the Emir praising Iran and calling for good relations with Israel while (contradictorily) backing Hamas and the Muslim Brotherhood.[8] The intrusion was followed by a massive distributed denial of service (DDoS) attack on Al-Jazeera, the Qatari-owned media outlet.[9] The news agencies in multiple Gulf States ran with the false story, leading to a diplomatic and economic blockade of Qatar by the UAE as well as by Saudi Arabia, Bahrain, Egypt, and Jordan.

In effect, the perpetrators of this campaign conducted a classic psychological warfare operation that undermined and isolated Qatar. Such incidents demonstrate how states are using cyber tools to mix the old with the new, as emerging cyber operations combine espionage, propaganda, economic warfare, and sabotage in an effort to signal resolve and shape adversary foreign policy.[10]

The Role of Cyber Operations in Conflict

The issue of how state and non-state actors use cyber operations alongside other coercive instruments has raised important questions about strategic preferences in future crises and conflicts. What role will cyber operations play in the major conflicts of the future? And what types of strategies guide how actors view the use of cyber operations in international crises and internal disputes?

These are important questions lacking a scholarly or policy consensus. Part of the problem is that the underlying technology is novel, constantly evolving, and secretive, all of which makes it difficult to study. In many cases, scholars have resorted to using concepts from previous eras, such as strategic nuclear deterrence, and applying them to cyber operations, though this approach has significant limitations.[11] Cyberattacks are considerably different from traditional 'kinetic' warfare: they do not involve direct force, do not (yet) destroy in the conventional sense of the word, and are difficult to attribute to specific actors.[12]

Adding to the confusion, technology-savvy programmers and engineers often understand the science but not the politics, while policymakers understand the politics but not the science. These challenges make it difficult to identify qualified experts or adequately train security specialists; they also have led to the development of poor cybersecurity products and inhibited the creation of clear political and military doctrines regarding cyber warfare.[13]

In most cases, questions about new doctrines and technologies can be resolved through trial and error in the real world. This is especially true in the domain of private-sector cybersecurity; companies continually invest and adapt to stave off threats or, if exploited due to a previously unknown vulnerability, rapidly reverse-engineer the attacking code and create a defense. This method allows security doctrines and technologies to adjust and adapt quickly and consistently.

Yet in the realm of interstate politics—especially at the level of grand strategy—such a solution is inadequate. States may have the luxury of adjusting and adapting to cyber espionage and one-off events, but such an approach does not sufficiently prepare policymakers for the potential role that cyber events might play in a fully coordinated military campaign. Large-scale political/military events—such as a great power crisis or war—would involve a range

of dynamic, largely unpredictable factors. Knowing how states and other political actors will employ cyber capabilities in crises and conflicts is difficult because we simply do not have enough 'cases' of such events taking place. In the absence of this data, it is extremely difficult to predict what is likely to occur.

Analytic Wargames as a Methodology

Analytic wargames represent a proven approach for assessing the potential outcomes of uncertain future events like cyber war. Wargames deal with choice in the face of incomplete information, and represent a sophisticated method for unpacking, understanding, and preparing for potentially significant multi-factor (but low-frequency) phenomena.

In developing analytic wargames, designers create competitive environments scripted around one or more specific scenarios. Players use resources at their disposal to meet their objectives and earn points based on their choices; referees help structure and guide the play in particular ways; and analysts make sense of the resulting data. Games are typically designed to allow players to creatively choose (within limits) what they can do.[14] By observing these games, recording their results, repeating play, and redesigning scenarios, analysts can use games to understand the nature of the complex and highly contingent problems the scenarios represent.

Analytic wargames are designed to be flexible and allow creativity in ways that computer simulations cannot; they allow observers to uncover strategies that might be otherwise unknowable. Players engaged in a game are not seeking to discover some analytic truth; rather they seek what will make them successful and enable them to win.[15] The players' process of seeking success leads them to use and combine resources in unexpected ways or adopt novel strategies (with referees determining whether or not such options are possible). This allows observers and researchers to gain greater analytic purchase on how actors might behave. By virtue of their interactive nature, wargames can generate new insights and lines of inquiry, and can help planners investigate the likely effects of changes in military doctrine or technology before making expensive investments.

Using Wargames to Assess the Role of Cyber Operations in Crisis

Given the covert character of contemporary cyber operations, wargames are particularly well suited for assessing the role of cyber operations in conflict. Our research applied the wargames methodology to reveal likely strategic preferences for the use of cyber capabilities where such capabilities are one tool in a broader coercive arsenal (e.g., economic sanctions, diplomatic threats, military mobilization and limited strikes, etc.).

History of Wargames

Gaming as a mechanism for projecting future outcomes has a long history, especially in military spheres. Analytic wargaming has its origins in 18th-century Germany with the development of "military chess," an expanded chess game that took place on a board with 1,666 squares, designed with the military in mind.[16] By the 19th century, the Prussian (and later, German) General Staff had incorporated Kriegsspiel (literally, "war-play") into their training and planning exercises.[17]

By the late 1800s, other armed forces recognized the value of wargaming, most notably the U.S. Navy, which made it an integral part of training at the Naval War College in Rhode Island. Since then, wargaming has expanded into many elements of the Department of Defense, academia, and the government.[18]

Wargames typically come in three general types: simulations, entertainment, or analytic. *Simulation wargames* are usually designed with the goal of testing and improving player skill in order to prepare them for similar real-life situations.[19] Games are precisely modeled with clear rules and built-in constraints. Simulation games are often used by the military to educate officers. By contrast, *entertainment wargames* are designed to be fun and put an emphasis on being "winnable" and balanced. Examples include common strategy games such as Diplomacy or Axis and Allies. *Analytic wargames* (such as those detailed in this report) are distinct in that the purpose of play is not to improve player ability or generate an enjoyable experience, but to help further the understanding of a phenomenon by observers and analysts, and to generate data that can be subsequently analyzed to improve and refine future planning. The national security community traditionally uses these games to test major operations, identify capabilities requirements, and analyze readiness levels and force posture.

We employed a two-level experimental design.[20] In the first phase, we developed a series of analytical simulations pitting participants in two distinct crisis contexts: 1) a dispute between rival great powers, called *Island Intercept*, and 2) an intrastate conflict between a government and domestic opposition, called *Netwar*. Both games allowed players to combine cyber effects with traditional forms of coercion in the security, political, and economic domains.

Phase I: The Games

ISLAND INTERCEPT

Island Intercept simulates a military crisis in the South China Sea, with two players representing either the United States or China. Both players are tasked with resolving a crisis regarding the Chinese capture of a Taiwanese ship in disputed waters.

How *Island Intercept* is Played

At the start of the game, a player is given a range of action cards, which fall into three categories:

- **Cyber Actions** generally allow players to snoop on their opponents, and subtly degrade their capabilities. Although the likelihood of success varies, these actions are frequently cheap and deniable.
- **Military Actions** are the most decisive types of actions with the biggest results; they are usually more expensive and politically restricted. Activity in this realm may negatively affect the political profile of a player's state, even if it does deliver results on the ground.
- **Political Actions** are taken to exert influence on other players or events. Players who ignore their leadership, regional allies, and world opinion will soon find their activity much more constrained than their opponent's.

The Scenario

Players in Island Intercept *were presented with the following scenario:*

Sixteen hours ago, the Tuo-River, a technologically advanced Taiwanese cruiser, was intercepted by a Chinese destroyer three miles off the coast of Uotsuri-shima, the largest of the disputed Senkaku/Diaoyu/Tiaoyutai Islands. Such interceptions are not uncommon and have usually ended without incident. This time, the situation has played out differently. Shortly after being hailed by the Chinese destroyer, the Tuo-River lost control of a number of its navigation, propulsion, radar, and sonar systems, rendering it immobile and defenseless. The Chinese destroyer drew up alongside the cruiser and demanded that it allow a boarding party on board in order to pilot the ship into international waters. The Taiwanese skipper refused the order.

In the short time since this event occurred, the situation has escalated. Officially, Taiwan has demanded that China immediately move its forces away from the Tuo-River and allow a Taiwanese ship to tug the disabled cruiser to a safe harbor. Taiwanese officials have also declared that they hold Chinese "electronic and cyber weapons" responsible for the Tuo-River's technical problems and

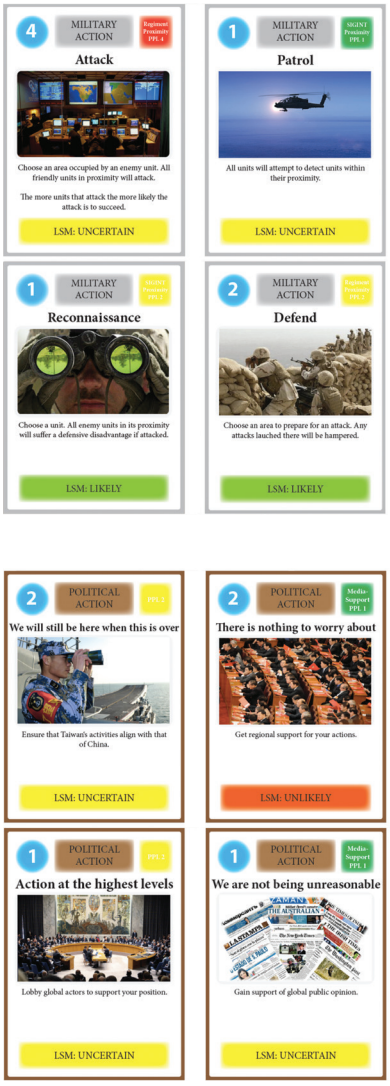
(*Continued on following page*)

(*Continued from previous page*)

demand an apology. Despite the official bluster, public opinion in Taiwan appears deeply divided, as commentators oscillate between demanding an armed response to China, or a complete acceptance of Chinese terms. It is uncertain to which of these constituents the Taiwanese government will respond.

China has claimed that it has nothing to do with the Tuo-River's immobilization, but nonetheless claims the right to board and tow the ship in order to "ensure safety in Chinese waters." This is seen by many as an excuse and that, if they tug the ship to one of their ports, Chinese personnel there will analyze the Tuo-River's secret weapon-systems.

While both the regional and international community are deeply uneasy with how events have played out, most have avoided any public statements, although the UN Secretary General has requested an emergency session. Only the United States has declared China's actions as "unambiguously aggressive" and has redirected a carrier fleet and other military forces to the area.



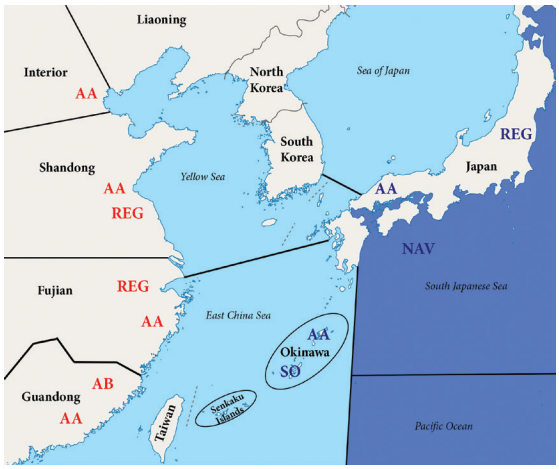
Players of Island Intercept *were provided with cards to explain the full range of choices they could make.*

A given action may require certain resources. For example, a player might not be able to make a move without a sufficient "political permission level" (PPL) or "proximity". Some cyber actions require network access, meaning the player must have previously gained access (through hacking or otherwise) to an opponent's cyber, political, or military network. There is also no guarantee that an action will succeed, thus every action has a "likelihood of success measure" (LSM) associated with it.

All actions also have a "detection level": whenever a player's action succeeds, it is possible his/her opponent will receive intel about the event. Some actions are detected immediately (such

as publicly debating in the United Nations or launching an attack), whereas others are more hidden (e.g., negotiating with allies, or cyberattacks).

Each side also receives a map that shows the region under dispute, the disposition of its assets in the region, and potential locations of opponent assets based on current intel. The map depicts three different types of area on the map: land, coast, and sea. Some military actions are limited to certain geographies. Cyber and political actions do not have any geographic restrictions.



The Controller map gives a high-level view of the game board; the information provided is limited based on each player's role.

Determining Outcomes

On each turn, a player attempts some (or no) actions, by outlining them on an order sheet that is passed to the controller (umpire). Between turns, the controller determines whether the player's (and his/her opponent's) decisions succeeded or failed by rolling a dice. After resolving the actions, the controller sends players a report with updates and the next turn begins. Each turn represents one week, and the game ends after three turns.

Results

In the course of eight games, both sides (U.S. and China) were less aggressive than expected, including in their use of offensive cyber operations. For example, Chinese players frequently pursued a "wait and see" approach, combining cyber espionage in an effort to determine U.S. intent while increasing more traditional intelligence activities, including military patrols and use of satellites and aerial reconnaissance. Other players chose to pursue a political path, lobbying at the international and regional levels. For example, a Chinese player initiated action at the United Nations and through regional forums, while assuming a defensive military posture and increasing their defensive cyber operations.

Notably, U.S. forces adopted a similar posture. Players tended to take diplomatic actions while positioning their military forces and seeking to gain advantage through cyber defense and espionage. Few players used paralyzing first strikes against mainland networks.

The Scenario

Players in Netwar *were presented with the following scenario:*

20XX. A global recession and political uncertainty lead to a new era of isolation, leaving regional powers to pursue their own agendas, often through coercive diplomacy and political, information, and irregular warfare.

A middle-income country struggles against corruption, low tax receipts, and protests to battle a violent extremist organization (VEO) linked to the paramilitary wing of a transnational criminal group operating a safe haven along the state's mountainous border. Weyland-Yutani Corporation, a multinational firm, is active in the country's mountainous border, developing the world's largest lithium mine. A transnational social movement of hackers and activists seeks to check the human rights abuses by the state and VEO as well as the predatory business practices of the Weyland-Yutani Corporation.

Each of these actors has a unique objective: the government wants to maintain its sovereignty; the VEO group wants to maintain its safe haven; the multinational firm wants unfettered access to lithium; and the activist network wants to speak truth to power.

NETWAR

Netwar is a four-player game that simulates the strategic interactions among a government, a violent non-state actor, a major international firm, and a cyber activist network, as each competes for domain advantage in three areas: the security sector, political and economic influence, and cyberspace. The player that has the advantage in the most domains at the end of the fourth turn is the winner.

Netwar has roots in Chaturaji, an ancient Indian form of chess involving four players. The game seeks to model the complex interactions that take place as governments confront violent groups—from Daesh/the Islamic State to transnational criminal groups—while also dealing with major international firms, such as Alphabet or ExxonMobil, and transnational advocacy networks like Anonymous, who use cyber tools as a means of coercing state and non-state actors. By using multiple, competing parties, the game seeks to model coordination challenges and diverging interests among various stakeholders in the digital space.

Players are randomly assigned to a team and assume a role. The government player represents a middle-income country currently trying to suppress a violent extremist organizations (VEO) operating along its border. The violent non-state player represents a transnational criminal network whose members are also linked to a violent transnational social movement. The business player represents a Fortune 500 multinational firm seeking to access mineral resources in the country. Last, the activist player represents a transnational advocacy network (e.g., Anonymous).

How *Netwar* is Played

The purpose of this game is to gather and analyze player decisions made during the course of a simulated multi-party competition. Each round represents three months; a game represents a year.

Each player has different resources from different sources. The government player relies on taxes. The VEO player has illicit activities and sympathizers (i.e., active and passive support). The business player—a Fortune 500 multinational firm—earns resources from revenue and controlling the board of directors and key appointments. The activist player, a transnational advocacy network, receives resources from active and passive support.

Players have access to different sets of actions. Only select actors can engage in physical attacks. All other players focus on defensive actions and competition in the political and economic domain and in cyberspace. In the political and economic influence domain, all four players compete to mobilize support for their cause and undermine their opponents through a mix of lawfare, sanctions, illicit networks, social media, diplomacy, and traditional propaganda. In the cyber domain, all four players can conduct offense, defense, and espionage in an effort to gain a position of relative advantage.

As with *Island Intercept*, the controller in *Netwar* collects movement sheets, calculates results, and communicates findings back to the players between turns. A player can only capture a domain through offensive action. To determine who wins a domain in a given round, the controller counts offensive and defensive points based on each player's moves. At the end of four rounds, the player who has made the most progress in the most domains wins.

Results

During the games, the state and violent non-state actor predominantly focused on progress in the security domain, conducting activities ranging from high-value individual targeting (i.e., drone strikes, raids) to terrorist attacks and seizing strategic villages. These actors often invested more in traditional security instruments of power rather than in cyber capabilities. Faced with violent threats and limited resources, they opted for brute force, as opposed to cyber coercion.

In contrast, the international firm and transnational advocacy network engaged in competitive strategy. They avoided security-sector competition, as they had little to no advantage in that space. The business players used a combination of legal action and lobbying—traditional forms of influence—and relied on cyber actions more to defend their networks. The transnational advocacy group, given the lowest resource base, focused predominantly on cyber capabilities, often seeking to exploit hidden information in adversary networks and using embarrassment to gain influence.

In the course of the game, players often followed a logic similar to that of Wikileaks, using the activist network to relay secrets about their enemies by "naming and shaming" or using outright distortion and propaganda campaigns. Cyber capabilities were a means of undermining adversary image and reputation, not a tool for launching attacks against critical infrastructure.

Phase II: From Wargames to Strategic Preferences

Once the sequences of both games were run, we analyzed the cyber strategies that the players employed, using the principles of war from U.S. joint doctrine,[21] as well as strategies from other spheres of competitive activity, including: security, political, economic, and cyber/information. Three primary strategic preferences for the use of cyber capabilities emerged:

- **Mass and objective:** *Use an escalatory cyber offensive to create a fait accompli*. Strike first using the ambiguity of cyberspace to undermine your rival.
- **Maneuver and surprise:** *Cross-domain escalation and brinksmanship*. Escalate in another domain (military show of force, economic sanction threat, diplomatic threat) to pressure your rival to sue for peace but wait to act in the cyber domain.
- **Economy of force and security:** *Test your opponent and limit escalation*. Probe your adversary with low-level cyber intrusions to signal resolve, but only retaliate at a higher level in cyberspace or in another domain if they strike first (tit-for-tat). Harden your networks (cyber defense).

Using these principles, we developed a *survey experiment*—a survey-based research method for identifying preferences around decision-making—to determine how larger numbers of participants would respond to the strategic preferences identified in the wargames.

We asked survey respondents to consider scenarios about crises similar to those depicted in *Island Intercept* and *Netwar*. We asked respondents to select the optimal strategy for each phase of the game. We varied the type of crisis (e.g., rival states, internal unrest), the actor (e.g., state, non-state), and control variables (e.g., relative power, issue salience, regime type, dispute type).

Phase III: Analyzing the Strategic Preferences

ISLAND INTERCEPT

We used Mechanical Turk to survey 1600 people about their preferred strategy in an emerging state-to-state crisis that involved cyber operations. The survey respondents were asked to assume the role of a great power. The experiment used four variations of the question to assess how behavior may vary based upon different levels of relative power (more or less than a rival) and issue salience (high or peripheral to your population).

State-to-State "Emerging Conflict"

In the first experiment, roughly 800 online survey respondents were presented with a variation on the following statement, with relative power and issue salience variables indicated in brackets:

You are a great power (i.e., United States, China, Russia) engaged in a dispute with a rival great power. The issue involved is of [*high or peripheral*] *interest to your population. You have* [*more or less*] *power than your rival and a history of militarized disputes that involve threats and displays of force short of war. Select the best strategy below:*

- **Mass and objective:** *Use an escalatory cyber offensive to create a fait accompli.* Strike first using the ambiguity of cyberspace to undermine your rival.
- **Maneuver and surprise:** *Cross-domain escalation and brinksmanship.* Escalate in another domain (military show of force, economic sanction threat, diplomatic threat) to pressure your rival to sue for peace, but wait to act in the cyber domain.
- **Economy of force and security:** *Test your opponent and limit escalation.* Probe your adversary with low-level cyber intrusions to signal resolve, but only retaliate at a higher level in cyberspace or in another domain if they strike first (tit-for-tat). Harden your networks (cyber defense).

During this dispute, actors disproportionately preferred an *economy of force and security strategy*: 52.3% of the 800 responses indicated a preference for this strategy. Neither relative power nor issue salience significantly affected cyber strategy preferences. Regardless of their position and the issue, *states preferred to take a cautious approach to using cyber operations to alter rival behavior in a crisis*.

State-to-State "Escalating Crisis"

In the second experiment, 800 survey respondents were asked about their preferred strategic response to an *escalating* crisis between state rivals; scenarios again included varying relative power levels and issue salience. Similar to the first experiment, economy of force and security still proved to be the dominant preference. Unlike the first round, *relative power concerns did shape strategic preferences*, but it was a weak relationship.[22] If an actor assessed a state as having more power, it increased the frequency of offensive responses (especially mass and objective) and lowered the number of economy of force and security preferences.

Key Findings from *Island Intercept*

The findings from this sequence of survey experiments are twofold. First, unlike in conflicts among state and non-state actors (i.e., the *Netwar* experiments), states are more likely to have a preference for exercising restraint and testing the resolve of rivals through limited cyber intrusions. Second, if a state determines that its opponent has stronger capabilities, this increases the likelihood that the state will escalate, but only in the cyber, as opposed to military, domain. This suggests that states may find mutual destruction to be so costly that no state believes its opponent will resort to it. In this way, the use of cyber operations in an escalating dispute may actually help stabilize strategic interactions between rivals.

NETWAR

In the surveys linked to *Netwar*, we evaluated the strategic preferences of domestic opposition groups engaged in an intrastate conflict. Different versions of the *Netwar* scenario were presented to players, based on whether they were state- or non-state actors, and based on different regime types (i.e., democratic, autocratic) and dispute types (i.e., ideological/religious, ethnic minority rights).

In the first survey experiment, non-state actors were presented with one of four statements, with variations as indicated by brackets:

You are an armed non-state actor engaged in a dispute with a [*democratic or autocratic*] *government over* [*ethnic minority rights or ideological issues, to include religious preferences*]. *The issue involved is of high interest to your constituents. You have enough power to hold terrain and challenge the government through protests, terrorism, and guerrilla attacks against government forces. Select the best strategy below:*

- **Mass and objective:** *Use an escalatory cyber offensive to create a fait accompli.* Strike first using the ambiguity of cyberspace to undermine your rival.
- **Maneuver and surprise:** *Cross-domain escalation and brinksmanship.* Escalate in another domain (military show of force, economic sanction threat, diplomatic threat) to pressure your rival to sue for peace but wait to act in the cyber domain.
- **Economy of force and security:** *Test your opponent and limit escalation.* Probe your adversary with low-level cyber intrusions to signal resolve, but only retaliate at a higher level in cyberspace or in another domain if they strike first (tit-for-tat). Harden your networks (cyber defense).

State actors were presented with similar statements, enabling them to pick one of the three strategies in response to a dispute with the non-state actor.

Unlike in the rival state experiments, strategic preferences in the state vs. non-state conflict surveys were more evenly distributed. *Economy of force and security* remained the preferred strategy, but only slightly, with 38.2 percent of respondents selecting this choice, compared to *mass and objective* (28%) and *maneuver and surprise* (33.7%). Controlling for regime type, both state and non-state actors took a more defensive posture when the polity was a democracy; if a regime was a democracy, the opposition was 16.9% more likely to take a defensive posture.[23] The type of issue driving the conflict (i.e., ideology or ethnic minority rights) did not produce observable differences in cyber strategy preferences.

In the second experiment linked to *Netwar*, the investigators evaluated the strategic preferences of *state* actors engaged in an intrastate conflict. Again, the results were more evenly distributed (*mass and objective*: 26.8%, *maneuver and surprise*: 30%, *economy of force and security*: 43.4%), and democratic regime types led to more defensive postures.[24]

Key Findings from *Netwar*

In all, this sequence yielded two important findings. First, states were roughly as likely to choose between the three strategies when in conflict with one another. This suggests that cyber warfare will complement, rather than replace existing strategy. Actors integrate cyber capabilities alongside more traditional approaches to shaping adversary behavior.

Second, democracies and non-state actors operating in democracies are likely to adopt defensive postures when engaging in cyber conflict. This is surprising because, while we might expect democracies to act with restraint, literature on terrorism suggests that non-state actors are more likely to be aggressive when operating in democracies.[25]

Implications for Policymakers and Military Leaders

Our wargame simulations suggest that cyber operations represent a 21st-century form of political warfare and covert action more than they do a military revolution. They convert the connectivity of the digital world into coercive leverage between political rivals. Cyber operations are not the domain of war or strategic escalation, but a competitive space in the shadows that political rivals use to achieve a position of relative advantage.

Additional findings that are most relevant to policymakers and military leaders:

- **Cyber operations do not replace strategy.** The inclusion of cyber operations alongside traditional instruments of statecraft and contentious politics is evolutionary, as opposed to revolutionary.
- **Fears of large-scale cyber operations may be overblown:** Many of the key influencers in the conversation around cyber operations promote a sense of alarm, yet our research suggests that the threat inflation is not necessarily warranted. Further research may be merited to determine whether institutions are investing too much in cyber deterrence and may want to shift the investment to other related priority areas, such as defense and authentication.
- **Cyber operations are a "use it and lose it" attack mode:** Actors may demonstrate restraint in using large-scale cyberattacks in part because of the relatively high probability of losing the ability to use a weapon once it has already been deployed; opponents (and others) can patch their networks once they identify a vulnerability. To employ cyber operations means that the crisis has to be so important that the actor will accept the cost of reducing, possibly to zero, the weapon's usefulness for the future. Cyber capabilities are also unique in that the vulnerabilities that make them effective (e.g., "zero-day vulnerabilities") do not appear with a predictable schedule or have clear effects prior to use.
- **Autocratic regimes are more likely than democracies to be the site of future cyber disputes.** The findings from our research indicate that the participation of an autocratic state makes the use of aggressive cyber operations more likely. This applied both in state-vs.-state and state-vs.-non-state contexts.

The Controller map gives a high-level view of the game board; the information provided is limited based on each player's role.

Finally, our investigation demonstrated that wargaming can help isolate frequently recurring postures and preferences in conflict situations—and can be a useful methodology for exposing likely preferences in cyber operations. In the future, we aim to continue testing major propositions linked to the cyber coercion literature about how cyber operations are becoming important tools for escalation management between rival states seeking to avoid deadly conflict.[26]

Endnotes

1 Thomas Schelling, *Arms and Influence*, (New Haven: Yale University Press, 1966), 2–6.

2 Eric Lipton, David Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *New York Times*, December 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0.

3 Benjamin Jensen, "The Cyber Character of Political Warfare," *Brown Journal of World Affairs* Volume XXIV, Issue 1, Fall/Winter 2017/2018.

4 Ashley Fantz, "As ISIS Threats Online Persist, Military Families Rethink Online Lives," *CNN.com*, March 23, 2015, http://www.cnn.com/2015/03/23/us/online-threat-isis-us-troops/index.html.

5 E.T. Brooking, "Anonymous vs. the Islamic State," *Foreign Policy*, November 13, 2015, http://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/.

6 Elizabeth Flock, "Anonymous Cancels Operations Against Drug Cartel, Say Kidnapped Member Has Been Found," *Washington Post*, November 4, 2011, https://www.washingtonpost.com/blogs/blogpost/post/anonymous-cancels-operations-against-drug-cartel-say-kidnapped-member-has-been-found/2011/11/04/gIQA11SzmM_blog.html.

7 Rebecca MacKinnon, "China's 'Networked Authoritarianism,'" *Journal of Democracy* 22, no. 2 (2001): 32–46; Jennifer Windsor, Jeffrey Gedmin, and Libby Lu, "Authoritarianism's New Wave," *Foreign Policy*, June 23, 2009, http://foreignpolicy.com/2009/06/03/authoritarianisms-new-wave/; Mathew Burrows and Maria J. Stephen, *Is Authoritarianism Staging a Comeback?* (Washington, DC: Atlantic Council, 2015).

8 Chris Bing, "What We Know and Don't Know about a Rash of Middle East Mystery Attacks," *Cyberscoop*, June 5, 2017, https://www.cyberscoop.com/know-dont-know-rash-middle-east-mystery-hacks/.

9 David Kirkpatrick and Sheera Frenkel, "Hacking in Qatar Highlights a Shift Towards Espionage-for-Hire," *New York Times*, June 8, 2017, https://www.nytimes.com/2017/06/08/world/middleeast/qatar-cyberattack-espionage-for-hire.html.

10 Brandon Valeriano, Ryan Maness, and Benjamin Jensen, "5 Things We Can Learn From the Russian Hacking Scandal," *Washington Post* (Monkey Cage), January 9, 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/01/09/5-things-we-can-learn-from-the-russian-hacking-scandal/?utm_term=.45fa54cdc7f0; Austin Carson, "Obama Used Covert Retaliation in Response to Russian Election Meddling. Here's Why," *Washington Post*, June 29, 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/29/obama-used-covert-retaliation-in-response-to-russian-election-meddling-heres-why/?utm_term=.be401e9f5445.

11 Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, 38, no. 2 (2013): 7–40.

12 Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence," *Foreign Affairs*, Nov/Dec. 2013.

13 Robert M. Lee and Thomas Rid, "OMG Cyber!: Thirteen Reasons Why Hype Makes for Bad Policy," *RUSI Journal*, 159, no. 5 (2014): 4–12.

14 Phil Pournelle, "Improving Wargaming in DOD," [Powerpoint Slides], 2015, retrieved from http://connections-wargaming.com/agenda/.

15 Jon Compton, "Wargaming! = Innovation: Searching for the Emergent Properties of Cat Herding," [Powerpoint Slides], 2015, retrieved from http://connections-wargaming.com/agenda/.

16 Roger Smith, "The Long History of Gaming in Military Training," *Simulation & Gaming* 41, no. 1 (2010): 6–19.

17 T.B. Allen, "The Evolution of Wargaming: From Chessboard to Marine Doom," in *War and Games* eds. T.J. Cornell and T.B. Allen (Rochester, NY: Boydell Press 2002).

18 Peter P. Perla, *The Art of Wargaming: A Guide for Professionals and Hobbyists* (Annapolis, MD: Naval Institute Press 1990).

19 Rosemary Garris and Robert Ahlers, "Games, Motivation, and Learning: A Research and Practice Model," *Simulation & Gaming* 33, no. 4 (2002): 441–67.

20 On the use of experimental designs in social science, see Rose McDermott, "Experimental Methods in Political Science," *Annual Review of Political Science* 5 (2002): 31–61, and James N. Druckman, Donald P. Green, James H. Kuklinski, and Arthur Lupia (eds.), *Cambridge Handbook of Experimental Political Science* (New York: Cambridge University Press 2010).

21 Current U.S. joint doctrine lists twelve principles: objective, offensive, mass, maneuver, economy of force, unity of command, security, surprise, simplicity, restraint, perseverance, and legitimacy. See Chairman of the Joint Chiefs of Staff, *JP 3-0, Operations* (Arlington: Department of Defense 2017).

22 The Chi Square test for independence was statistically significant ($p < .01$) but the Cramer's V was .166 (less than .2), indicating a statistically significant but weak relationship. Because the experiments dealt with nominal, non-parametric data and independent samples with mutually exclusive categories, a Chi-Square test and Cramer's V were used.

23 The ratio is based on a risk analysis. The defensive cohort, made by differentiating strategies between offensive (mass and objective, maneuver and surprise) and defense (economy of force and security), returned a risk ratio of 1.169.

24 Risk estimate = 1.53. It should be noted, though, that relationship is weaker (Cramer's V = .183) but still statistically significant ($p < .01$).

25 Andrew Kydd and Barbara Walters, "The Strategies of Terrorism," *International Security* 31, no. 1 (2006): 49-80.

26 Brandon Valeriano, Benjamin Jensen, and Ryan Maness, *Cyber Coercion: the Evolving Character of Cyber Power and Strategy* (New York: Oxford University Press 2018).

About the Authors

Dr. Benjamin M. Jensen holds a dual appointment as an Associate Professor at the Marine Corps University, Command and Staff College and as a Scholar-in-Residence at American University, School of International Service. At Marine Corps University, he runs an advanced studies program, the Gray Scholars. The program integrates student research with long-range studies on future warfighting concepts and competitive strategies in the U.S. defense and intelligence communities. His book, *Forging the Sword: Doctrinal Change in the U.S. Army, 1975–2010*, was published by Stanford University Press in 2016. His second book, *Cyber Strategy: The Evolving Character of Power and Coercion*, will be published in May 2018 by Oxford University Press. His third book, co-authored with Lieutenant General Charles Cleveland, *Military Strategy in the 21st Century: People, Connectivity and Competition*, will be published in summer 2018. Dr. Jensen also writes a column on the changing character of conflict for *War on the Rocks*, entitled "Next War." Dr. Jensen is an alumnus of the Philip Merrill Center for Strategic Studies Basin Harbor Workshop, the Bridging the Gap Initiative, and the American Academy for Strategic Education. Dr. Jensen has written opinion pieces on the changing character of war for the *New York Times*, *Financial Times*, *Washington Post*, *Washington Times*, *USA Today*, *U.S. News and World Report*, *Philadelphia Inquirer*, *Al-Hayat*, and the *Daily Star*. His media appearances include BBC, Fox News, National Public Radio, and Canadian Television. Dr. Jensen has also supported multiple U.S. government agencies including contributing to Joint Staff studies and war games on transnational threats and great power competition, counterinsurgency doctrine, intelligence community scenarios on the future of Afghanistan, studies on cyber operational art, and red team assessments for the NATO headquarters in Afghanistan. He is a Non-Resident Senior Fellow at the Atlantic Council.

David Banks is a Professorial Lecturer at American University, where he focuses on international order, great-power politics, and diplomacy. He holds a Ph.D. in Political Science from George Washington University and an M.A. in Global Governance from the University of Delaware. His dissertation research investigated the motivation for, and political consequences of, state violations of diplomatic practice. He has begun work on a large research project that compares the great-power treaty-systems of the 19th century with those of today. In addition to these projects he has number of articles under review or in development regarding diplomatic practice, symbolic diplomacy, coercive diplomacy, and great power conferences. He has been published in *Time*, *The Independent*, and *U.S. World News & Report*.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley