MARCH 2021

Toward a More Coercive Cyber Strategy

Remarks to U.S. Cyber Command Legal Conference, March 4, 2021[1]

By James A. Lewis

The United States is on the defensive. For more than 12 years, our great power opponents have held the initiative and scored success after success, while the United States remained in a reactive posture. These opponents have had their share of failures, but particularly in cyberspace, which is a focal point for conflict today, they have had an open field for action. The topic before us is how we can change this.

Two episodes from history provide a starting point for our discussion. In 1915, when it was clear that World War I would not end quickly, Henry Ford filled a ship with pacifists and academics and set sail for Europe to persuade the warring powers to renounce conflict. The appeal was not well received. Current desires of the private sector for a digital peace are similarly unlikely to meet with success. Cyber conflict does not occur in a political vacuum. It is a conflict between states. When nations are not interested in peace, any appeal—no matter how impassioned—will fail, and while it is important to involve the private sector and civil society in cyber strategy, we should be clear-eyed about the unwillingness of our major opponents to end hostile actions.

Twenty years later, in a 1935 House of Commons debate over the Royal Air Force budget, a member of parliament said there was no need to spend money on new military capabilities as Herr Hitler had renounced aerial bombardment. This was overly optimistic. Opponent intent is better gauged by actions than by words. Both incidents show the reluctance of democracies to acknowledge conflict, which of course makes conflict much harder to avoid.

[1] Remarks as prepared. The recording is available here: https://www.dvidshub.net/video/785814/cyber-policy-expert-speaks-2021-uscybercom-legal-conference.

The interconnections and dependencies created by globalization also make it harder to recognize how the international environment has changed for the worse in the last decade and that relations among great powers no longer follow peacetime patterns or rules. While we are not in full conflict today, we are also no longer at peace.

Historical analogies are always imperfect. These analogies are imperfect because a major difference between the wars of the last century and now is that while nations are already engaged in conflict, the nature of conflict has changed. Wars no longer begin with formal declarations or dramatic kinetic actions. Conflict with major powers today is largely nonmilitary. These differences make it easy to fail to notice the deterioration in our security. There is some debate about whether to call the new environment conflict or a competition, but in cyberspace, it is conflict where opponents routinely violate U.S. sovereignty and use coercive actions to harm our nation.

This makes an important first step for a new cyber strategy to admit that we are already in a conflict with powerful authoritarian opponents. Their goal is to damage the United States and restructure the global order to better serve their own interests. Simple metrics can guide our assessment of cyber strategy. An initial metric is that if opponent actions have decreased, the strategy is working. By this measure, our current strategy does not work.

A second important step is to ask if strategic precedents from the twentieth century and especially from the Cold War are still useful. A strong case can be made that they are not. Nuclear war was the centerpiece of late twentieth century strategy. Nuclear weapons, especially after massive arsenals had been accumulated, posed an existential threat. This meant their use was unthinkable. You may recall the film *War Games*, which concluded there are no winning moves in nuclear war. In that environment of existential threat, a strategy of deterrence made sense. That construct remains powerful among a generation of strategists whose views are shaped by the Cold War—indeed much of the lexicon of cyber strategy is drawn from the Cold War.

But these Cold War ideas are inadequate. This is not a bipolar contest and both the techniques and the aims of Russia and China differ from those of the Soviet Union. Cyber conflict does not pose an existential threat. This increases opponent willingness to accept risk and decreases their incentives for negotiation. A nuclear exchange would have produced millions of casualties in a few minutes. Cyberattacks cannot match this and media efforts to inflate cyber risk are unpersuasive. In the absence of an existential threat or even the risk of the significant damage that armed conflict brings, there is little incentive for opponents to make concessions on the use of coercive cyber actions or to stop using them.

The nature of conflict has changed in ways that highlight the importance of cyber operations. One of the most important changes is the limits on military action created by nuclear weapons. Another is the use by opponents of the coercive opportunities created by networks. This new kind of conflict is ambiguous and less reliant on conventional military actions, and we lack the analytic tools needed to reconceptualize strategy for it.

A military audience knows why having the initiative is important and preferable to being reactive. The pursuit of one Cold War strategic concept, deterrence, helps explain why we have yielded the initiative to our opponents. There have been many attempts going back more than a decade to revive deterrence to fit the cyber environment. Despite these efforts, we have not found the right formula. This is because it does not exist. Hostile incidents continue to increase in number, and while the ultimate goal of deterrence—which is to prevent conflict—remains worthwhile, it is not achievable in the current environment, where opponents have decided on a course of confrontation. We need to ask how we ultimately return to a situation of stable relations with opponents, get them to reduce their hostile actions, and decrease the risk to our interests in cyberspace. Deterrence will not achieve this.

Opponents also have the initiative because the United States lacks a coherent strategy. What are our strategic objectives? Making the world safe for democracy did not work out so well. Regime change in Moscow or Beijing is beyond our capabilities and did not succeed in less powerful countries. Stability is the wrong goal when opponents seek to change the status quo. The need to rethink global strategy helps explain why we are on the defensive in cyberspace, and constant appeals to deterrence seem to indicate a certain lack of innovation in strategic thought.

The decade after 1990 was a period when the United States had the luxury of being apparently unchallenged. We did not need to win. This is no longer the case, but our thinking has been slow to adjust. A new approach must discard deterrence and identify the goals we wish to achieve in ways that are actionable. We have not deterred our chief opponents from malicious cyber action.

It is comforting to argue that there have been many successes that are not public, but this can be challenged on two grounds. First, if the battle is over perception and public opinion, secret successes contribute little. Second, while we may have exquisite knowledge of Chinese and Russian military capabilities, it is exquisite knowledge in support of an outdated strategy. Precise knowledge of Russian strategic forces' readiness and deployments is not actionable and of secondary importance in today's engagements. We know from hard experience that many tactical victories in pursuit of an unworkable strategy do not add up to success.

We need a different approach to change opponents' calculations of the benefits of action against the United States. The Biden administration has made a good start with the president's public messaging. He said, "I made it clear to President Putin, in a manner very different from my predecessor, that the days of the United States rolling over in the face of Russia's aggressive actions—interfering with our election, cyberattacks, poisoning its citizens—are over." On China, he said, "We'll confront China's economic abuses; counter its aggressive, coercive actions; to push back on China's attack on human rights, intellectual property, and global governance."

These are the right messages, but those who have engaged with the Russians and Chinese know that they will first take a wait-and-see approach and then decide to test the new administration. Words and messaging are important, but not by themselves sufficient. The immediate requirement is to develop and execute appropriate responses that go beyond words. Much of this task falls on Cyber Command and we can build on Cyber Command's successes. Today, I will discuss ideas for what a cyber strategy for the new environment of intangible conflict could look like.

Our opponents are unlikely to abandon confrontation with the United States, but we can improve the terms of conflict. While opponents will exploit the United States' political divisions, a new cyber strategy can help shield the Republic until these are resolved. An immediate strategic goal is to reduce the number of malicious actions by opponents against U.S. targets. Another is to defend allies, and a third is to bring opponents to negotiate the terms of a less dangerous cyber environment.

To do this, we will need a more assertive strategy that is based on how to achieve strategic effect using cyber actions, how to coordinate with allies, and how to manage risk. Cyber strategy must be embedded in our larger China and Russia policies, and coercive actions must support and drive toward larger national objectives for relations with Russia and China rather than being blindly reactive. Domestically, a new cyber strategy must be accompanied by public messaging and by building both stronger defenses and greater resilience for when defenses fail.

One way to define strategic effect is to look at what opponents consider it to be. Their primary concern is political, that the United States will trigger some kind of Arab Spring or color revolution in their countries. The second concern is that we will use cyber capabilities, in combination with other advanced conventional weapons, to cripple both their command and control and their own strategic assets. They believe that their deterrent forces do not protect them, since the United States can produce strategic effect without crossing the nuclear threshold that would justify their own use of nuclear weapon. From their perspective, strategic effect is disrupting political leadership, command and control, and strategic military capabilities.[2]

The Obama administration did much to advance cybersecurity in the United States by organizing the executive branch and in developing a first national strategy, but it was tested by foreign opponents and found wanting. A defensive strategy will not stop well-resourced, persistent, technically skilled, and aggressive opponents. Better network defenses and private sector actions are important, but by themselves, they are the digital equivalent of the Maginot Line.

The alternative to the Maginot Line is maneuver warfare. There is a general recognition that an effective strategy requires altering opponents' calculations of the risk of acting against the United States in cyberspace. Doctrinal disputes over whether this is deterrence, dissuasion, compellance, or some other twentieth century concept qualify as ancestor worship. The core of a new strategy is achieving coercive effect by using cyber actions against opponents to reshape their calculations. These effects could be tangible or intangible but will require either the use of force or the threat to use force. We will need to identify the right targets and the right level of damage to achieve strategic effect. The United States has been on the defensive, but it is in our power to change this.

The definition of force in cyberspace is complicated and not fully agreed upon, but at a minimum, it means inflicting damage, either tangible or intangible, on the opponent. Other non-forceful actions, such as sanctions and indictments, also have effect but are unlikely to change opponents' risk calculations. Sanctions are ineffective against Russia, which has become inured to them, and not sufficiently harmful to affect China. Indictments, while painful, are too narrow in their effect. Anything short of a forceful response is likely to go unnoticed by opponents who are no strangers themselves to the use of force and threats and expect it to be a normal part of the exercise of power.

This idea of a more assertive strategy that incorporates coercive elements will make many uncomfortable, but defensive actions have proven inadequate. This is a dilemma for U.S. society, which has become more risk averse. Our preference to avoid risk can shape strategies in ways that give our opponents an advantage. Fears that an assertive strategy will lead to tit-for-tat exchanges that will escape our control ignore the fact that our opponents are already engaged in aggressive actions and they see our repeated failure to respond as a green light for continued and more damaging action in cyberspace.

There is increased risk in adopting a more assertive strategy, but a risk-averse strategy has failed. Any new strategy must accept risk and develop the tools to manage it. The most important of these are managing escalation risk, messaging, and alliance building.

The risk of escalation is grossly exaggerated. Countless Track II dialogues are undertaken to reduce the risk of miscalculations that could lead a cyber incident to escalate into kinetic violence. Yet, in two decades of

[2] This paragraph was not included in the delivered remarks.

malicious cyber action, there has never been an incident that has led to escalation. While there have been a few instances of unintended consequences and collateral damage, these did not lead to an escalation of conflict. We can now reject the initial hypothesis of miscalculation and escalation as inaccurate. The likely reasons there have been no cyber incidents that resulted in escalation is that states maintain careful control of their most dangerous cyber capabilities and have devoted their own strategies to reduce risk. We should learn from their experience of tight leadership and control as we design our own active policies.

A new strategy must use communications, messaging, and signals with opponents, allies, and publics. This does not mean that every action should be accompanied by a press release, but a new cyber strategy will need to use public and private communications to shape opinion in ways favorable to the United States and make it clear that our actions are guided by international law and agreement. Adopting a more assertive posture in cyberspace is in itself a message that will improve our position with opponents. Diplomatic and public messaging can help manage escalation risk and strengthen collective responses with allies while shaping opponents' planning. Decisions on timing and audience will be determined by the specifics of each action, but our overall goal should be to end Strangelovian opacity.

Building and maintaining alliances and communicating with publics and opponents will require addressing issues of evidence and attribution. To quote a European colleague, our allies cannot go to their parliaments and publics and say, we are taking an action on the basis solely of U.S. statements. Echoes in Europe of 2003 still hang over our intelligence assessments. This means that to create a coordinated response to opponents, the United States will need to find mechanisms for greater intelligence sharing. In the past, the chief limitation on intelligence sharing was to protect sources and methods. This remains important, but an overly protective approach to intelligence sharing will not win us the support needed in this contest.

The United States has done good work in laying the foundation of an informal coalition of like-minded states with the September 2019 Joint Statement by 28 nations on advancing responsible state behavior in cyberspace. These countries agreed to "work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law." This will not be a formal alliance nor can we expect those who decide to participate to join us on every occasion, but one clear advantage over our opponents is that we have allies, even if those alliances must be repaired after the damage of the last four years.

The 2019 cooperation statement builds on the 2015 UN norms, which created a framework for responsible state behavior in cyberspace. Norms provide the basis for a collective response to actions that violate them. Although these norms were endorsed by all UN member states, our opponents have chosen not to observe them. Remedying this requires the imposition of consequences. Norms are still essential because a more assertive and coercive cyber strategy needs to be based on and justified by the need to create costs when norms are ignored and because we will ultimately need an agreed normative framework that nations observe if we are to reduce conflict.

Target selection and careful graduation of effect will also help manage risk. We can divide targets in general categories of civilian, critical infrastructures, political infrastructure, tangible military assets, and cyber capabilities. Each has different legal requirements. Some targets can be dismissed immediately. Attacking purely civilian targets would be contrary to our obligations under international law and produce no strategic benefit.

While attacks on critical infrastructures are permissible under international law and agreed norms and despite all the discussion of cyberattacks on critical infrastructure, there is little strategic benefit in attacking them. A truly crippling attack would provoke a powerful response from the opponent. This is why Russia and China have not attacked U.S. critical infrastructures. They have probed infrastructure, conducting the reconnaissance necessary for attack, but this is to create and maintain cyber capabilities, like building missiles but not launching them. Much of our understanding of strategic effect still relies on concepts drawn from airpower and strategic bombing. While these topics lie outside the scope of this discussion, we know that the current conflict is not like World War II, and neither the United States nor its opponents are trying to cripple industries.

Attacking opponent political infrastructures could be usefully coercive. This does not mean attempting to tamper with their voting machinery, which would be a waste of time and effort, but exposing the mechanisms of influence and control used by Russian or Chinese political elites. It could also mean information operations to expand discontent—this would be particularly effective against China. But such actions would need to be carefully calibrated because efforts undermining their regimes are what our opponents fear most and could trigger a more aggressive response.

For example, when a U.S. media outlet published the details of the wealth illegally assembled by a Chinese leader's family, there was a prompt and aggressive response as the Chinese sought to find the source of the leaks, identify links to the U.S. government, and punish the media outlet. The fragility of opponent regimes, whose greatest fear is their own populations, means political actions will produce a neuralgic reaction greater than what is needed for coercive purposes.

Political interference could be used in small doses to make the point of coercion, but a sustained campaign to undermine opponent governments, as Russia has done to us, would only make sense in the context of a decision about what we want in our relationships with them. Is the goal to replace current leaders or to use specific actions as cautionary examples to dissuade them? Before using political action, we need to decide what it is we want to achieve with those countries.

This leaves actions against opponents' cyber capabilities as the most compelling target set. This is consistent with other areas of military doctrine, where degrading an opponent's capacity to operate and attack is an essential first step in any campaign. Damaging the cyber infrastructure that provides an opponent the ability to engage in espionage or politically coercive actions is most likely to benefit the United States while minimizing the risk of escalation.

To draw on historical examples, when the Luftwaffe concentrated on destroying British aircraft and bases in 1940, it was on track to win the Battle of Britain. When it switched to civilian targets, it lost. A similar issue for the U.S. Army at the onset of the North Africa campaign was whether air units should be dedicated to support ground units or focus instead on destroying Luftwaffe. The answer became clearer in air battles over Europe, where fighter-bomber sweeps against Luftwaffe forces were more effective than strategic bombing at degrading opponent capabilities. While there is still some debate over these histories, the lesson we can draw from these examples is that damaging an opponent's ability to operate in cyberspace is the best course of action.[3]

A strategy to do this requires decisions about pacing, targets, scale, the degree and kind of pain and damage inflicted, and the permanence of any effect, but these variables can be manipulated as experience is gained and adjusted in light of experience. A campaign to degrade opponent cyberattack capabilities can help define the limits of acceptable action in cyberspace and would be the equivalent of the "border clash-

[3] This paragraph was not included in the delivered remarks.

es" and maneuvers used by nineteenth-century powers to signal priorities and interests. It is likely that opponent political leadership will feel less threatened by actions against their cyberattack infrastructures and will not perceive this as creating the same level of risk as would be the case if the objective was other political or strategic capabilities.

One question to consider in developing an assertive and coercive cyber strategy is the value of preemptive action. Preemption assumes that we have advance knowledge of specific opponent planning and can choose to warn an opponent that we know or seek to disable them. This kind of advance knowledge is a rare commodity, however. Because surprise and speed are the essence of the final phase of cyber actions and given that many actions are undetectable for months, preemption seems unworkable.

An alternative to preemption could be loosely termed "armed reconnaissance," expanding defend forward and persistent engagement to undertake intrusive cyber operations to locate and attack targets of opportunity. This could be part of a campaign plan for attacking opponent cyber assets in an incremental and sequential manner to degrade their capability to attack the United States and its allies.

Operational pacing is one way to manage risk while still signaling opponents on the boundaries of acceptable behavior. The best approach may be an intermittent series, with pauses to observe opponent reaction and to appropriately communicate intent, rather than a continuous sequence of actions. Intermittence also reduces the risk of expanded conflict, but pace and rhythm in a more assertive strategy need further consideration.

Another question involves proportionality. Responsive actions must be proportional to opponent action both to meet our obligations under international law and to manage the risk of expanded conflict. But proportionality remains unclear in cyberspace. What is the proportional response for election interference? Defining proportionality will require a period of trial and error because cyber actions blur the lines between military, espionage, and political warfare in ways that require adjustments to our thinking, doctrine, and tactics.

This blurring means that the community of nations may need to reconsider the formal and informal rules that apply to espionage. The immense increase in the opportunities for spying brought by network technologies also points to the need for some reconsideration. There are precedents for constraints on espionage as part of a larger alliance strategy, but this requires a complex discussion of the benefits and risks of constraint, and only makes sense as part of some larger diplomatic effort.

Moving to a more assertive cyber strategy does not mean that we are about to launch cyber war. It does not preclude efforts to reestablish serious engagement at senior levels with our opponents. It means changing the emphasis of our strategy and actions from trying not to lose to trying to win. The bulk of the action will still be diplomatic, but this can be sharpened and made more persuasive when accompanied by demonstrations of coercive effect or the threat of coercive effect.

Because we cannot reasonably expect to defeat our opponents, our goal must be to reach some understanding with them of what is no longer acceptable in cyberspace. Using coercive actions to improve one's negotiating position is a long-standing diplomatic practice and an achievable objective for a new cyber strategy. Meaningful negotiation with our opponents is not possible in the near term—they are not interested in serious engagement and we have a credibility deficit—but if we pursue an assertive strategy that includes coercion, we can eventually bring them to the table.

The United States did not have a credibility problem in the Cold War because of the immense destructiveness of nuclear weapons—something that cyber lacks—and because when Eisenhower chose deterrence, the United States had already used nuclear weapons, firebombed cities, and had a demonstrated commitment to the doctrine of strategic bombing. History and experience shaped opponents' risk calculations. These are lacking today. Perhaps after a more coercive strategy has been in place, we can arrive at an uneasy stability in cyberspace, but there is little incentive for opponents to now agree to this. If your goal is to change the status quo in ways that favor your national interests, you will not be interested in stability. Rebuilding U.S. credibility in cyberspace to create the foundation for agreement requires action.

In any negotiation, the United States will not get everything it wants. Our opponents will not observe human rights or the rule of law, as they regard these as unjust violations of their sovereignty. Their actions at home and in foreign countries demonstrate this. Our pursuit of these objectives must use other techniques. But we can improve our situation in cyberspace with a new strategic approach based on coercion or the threat of coercion since we are in conflict with powerful and unscrupulous opponents.

This discussion has sketched out possible new directions for strategy but leaves many open questions. Some can only be answered in light of experience. We know that the ultimate test for doctrine and strategy is actual engagement with the opponent. How coercive we will need to be, what form it should take, what messages should accompany it, and how much time is needed for opponents to recalculate in light of a more assertive approach are open questions, but a new strategy cannot shy away from coercion and credible threats. We need to identify cyber actions that create strategic effect, ensure this is consistent with our obligations under international law, coordinate with allies to achieve this, and communicate our intent to our publics and opponents.

There is risk in this kind of new strategy, but risk is unavoidable if we seek change, and risk can be managed. Cyber conflict is messy, usually covert, and often ambiguous. Better cybersecurity requires persistence and boldness. Cyber Command has built the tools. As a nation, we now need to decide how best to use them in defense of ourselves and our allies. ■

***James Andrew Lewis** is a senior vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.*

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).