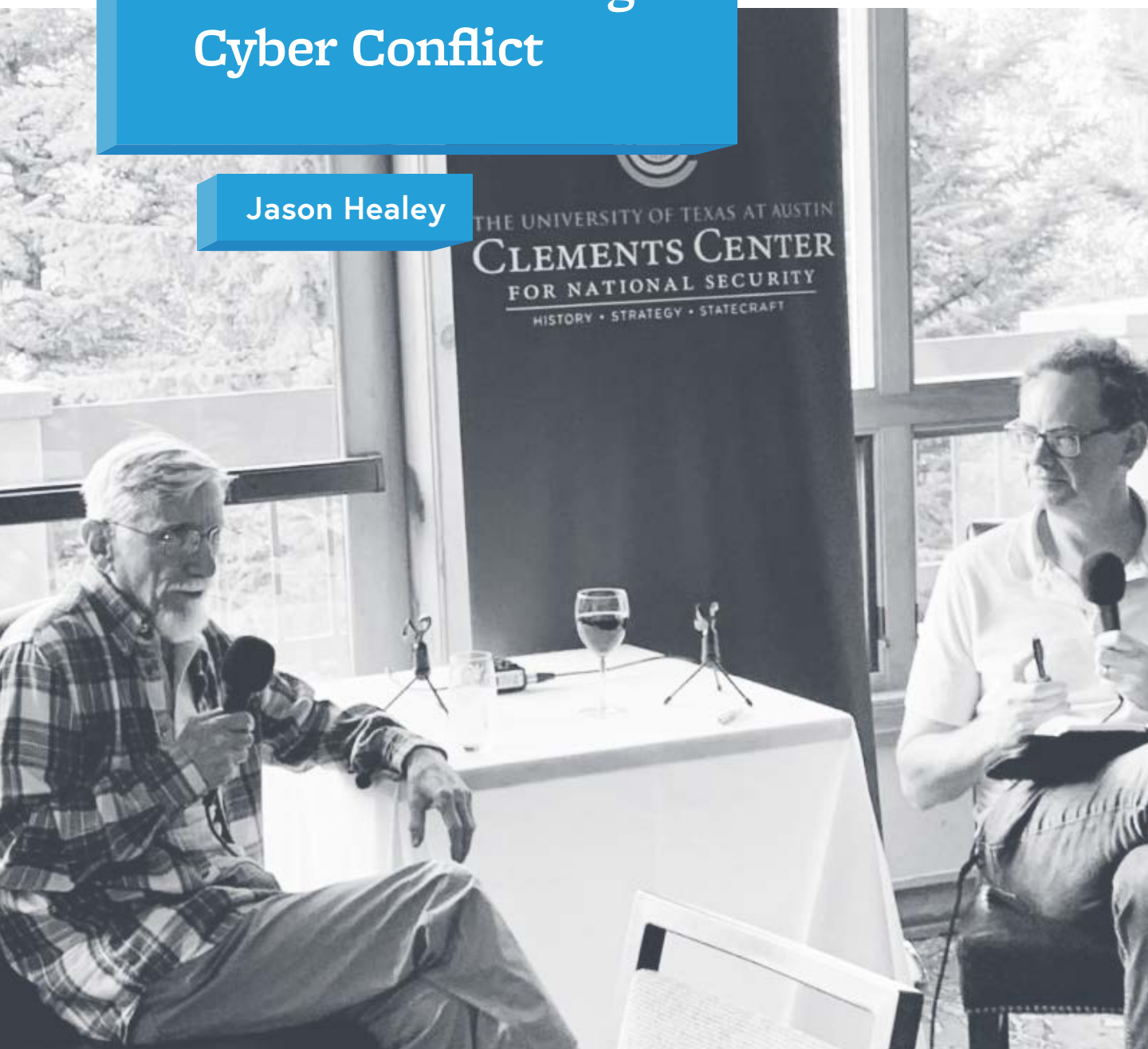
Texas National Security Review: Volume 5, Issue 3 (Summer 2022)
Print: ISSN 2576-1021 Online: ISSN 2576-1153

# Bob Jervis' Impact on Understanding Cyber Conflict

Jason Healey



In this roundtable feature, Jason Healey reflects on Bob Jervis' contributions to cyber conflict research and on their collaboration over the years.

Bob Jervis made important contributions to research on cyber conflict because he knew that, although it was fought using new kinds of tools, it was still conflict. Bob's instincts — formed by decades of research and interaction with policymakers — told him that cyber conflict was dynamic and incredibly complex, with humans on either side, including military, intelligence, and political leaders. Such a conflict would be driven by many of the same dynamics, emotions, miscalculations, misperceptions, and cognitive errors as conflicts that are fought on more traditional battlefields.

These conclusions led him to be cautious, if not downright doubtful, about theories and strategies like U.S. Cyber Command's "defending forward," which argue that the only path to security and stability in cyberspace is to reduce operational constraints.[1] U.S. cyber forces must be able to "maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations."[2]

These types of strategies seemed perhaps a bit too self serving and simple to Bob. Sure, such operations might intercept and slow down adversaries. But would our shots truly get an adversary to step back and not just temporarily keep its head down? As Jack Levy put it, more generally, in his tribute to Bob,

> Building on theories of complexity, Jervis emphasized that everything is connected to everything else; that 'we can never do merely one thing'; that causal relationships are often interactive; that non-linear relationships, third-party behavior, and negative and positive feedback generate unintended consequences; and that actors co-evolve with their environments.

In Bob's view, pushing back against cyber adversaries, as U.S. Cyber Command asserts is an imperative, seemed accordingly unlikely to lead to long-term stability, regardless of the amount of agility, skill, or persistence applied.

Too many cyber theories and strategies appeared to be rooted in narratives of the intransigence and brazenness of cyber adversaries, requiring the American military accordingly to adopt yet looser rules of engagement (and not coincidentally larger budgets). This struck Bob as all a bit contrived, a re-telling of history with the United States recast as the plucky underdog instead of the entitled rich kid (and occasional bully) enjoying the perks of playground hegemony.

Cyber conflict was his beloved *Rashomon* being played out yet again, with each participant having a widely differing view of even the most basic facts in an unfathomably complex system, leading to misperception, miscalculation, and yet more complexity.[3] "What each player does influences not only specific responses by others," he wrote in 2016, "but many of the contours that will guide future play."[4]

More importantly, he wondered under what set of circumstances U.S. cyber operations would get adversaries to reverse course to accept American norms and stability? The "uncertainties and ambiguities ... and lack of shared understandings about what would constitute escalation," he wrote, should give policymakers substantial doubts about any particular path to deterrence or stability. They should be especially leery about a strategy that depends almost entirely on yet more U.S. cyber operations that America's adversaries — whose blood is up just as much — are supposed to recognize as defensive and stabilizing.

I didn't know of Bob's concerns when I became his colleague at Columbia University's School of International and Public Affairs in 2015. Few people of his generation could get their heads around cyber issues (Joe Nye of Harvard is one of the other most-prolific outliers). I knew Bob would be different when, in my first months at the storied Saltzman Center for War and Peace Studies, I knocked on his office door to talk about spiral escalation in cyber conflict, a topic we would write about years later. I was surprised to hear him say, "Ah yes, like Olympic Games," using the formal name for the joint U.S.-Israeli operation that resulted in the

1 "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," United States Cyber Command, April 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

2 Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Forces Quarterly* 92, January 2019, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1736950/a-cyber-force-for-persistent-operations/.

3 Robert Jervis, *How Statesmen Think: The Psychology of International Politics* (Princeton, NJ: Princeton University Press, 2017).

4 Robert Jervis, "Some Thoughts on Deterrence in the Cyber Era," *Journal of Information Warfare* 15, no. 2 (2016): 66–73, https://www.jstor.org/stable/26487532.

Stuxnet attack on Iran's nuclear enrichment program. I'd not expected him to be so well read in cyber conflict and to be familiar with such details. It was the first time he showed that his understanding went below the headlines.

## Collaboration

Bob was famous for his wit, patience, and willingness to mentor the upcoming generation of scholars. I was not the only one who would knock on that door looking for advice, guidance, or his opinion on some thorny topic. He always attended the School of International and Public Affairs' cyber workshops and was especially keen to join the ones that featured younger scholars, where he could see the latest methodologies. Still, the cyber academics who he kept closest — such as J.D. Work, with his encyclopedic memory of who hacked whom — were those with long careers as practitioners, rich with knowledge beyond what was printed in journals.

One of my greatest personal joys was when he and I agreed on just how dangerous cyber conflict could be. Building on his 1978 classic "Cooperation Under the Security Dilemma," Bob noted that it wasn't just "doubly" dangerous, but "quintuply" dangerous, or worse. This early connection of his previous work with cyber issues led us to surmise that there were all sorts of hidden and misunderstood dynamics of cyber conflict.

The Minerva Initiative of the U.S. Department of Defense agreed, and funded Bob and me for a three-year exploration of these dynamics. Out of this time of exploration grew all of our subsequent thinking and publications on cyber conflict, even those that took place outside of the original period of this generous funding. As discussed more below, there are many more insights from our collaboration during this time that are yet to be published.

The highlight of our work together was a paper titled "The Escalation Inversion and Other Oddities of Situational Cyber Stability," published in 2020 in the *Texas National Security Review*. The goal of the paper was to move away from asking "whether" cyber operations are escalatory or de-escalatory (a false binary of much past research on this and other dynamics), and instead to ask "under what conditions" it might be one or the other.[5] Bob brought a deep appreciation of history to his work, so we were a natural fit, as I'd published the first history book of cyber conflict.[6] We both suspected that the escalatory nature of cyber operations would depend at least as much on the geopolitical tensions between adversaries as on the technical characteristics of cyber capabilities.

The result of this first collaboration was a recognition that there were at least four different escalatory mechanisms. The one with the most academic currency was how cyber capabilities can act as a "Pressure Release." Because their effects can be both reversible and non-lethal, their use will often defuse geopolitical crises, findings that are associated with the work of other academics like Josh Rovner, Ben Jensen, and Brandon Valeriano.[7] However, we were perhaps the first to highlight that this is only true in times of relative peace and when *both* rivals strongly want to limit conflict. We were in even newer territory with the three other escalatory mechanisms that we proposed: what we called "Spark," "Pull Out the Big Guns," and the "Escalation Inversion."

For more than three decades, cyber conflict has been intensifying over increasingly existential issues and so might trigger an acute geopolitical crisis, a scenario we called "Spark." Perhaps the best example so far is the pressure on U.S. policymakers to stop Russian ransomware gangs, especially after the attack on Colonial Pipeline.[8]

Pull Out the Big Guns (a name that neither of us was ever happy with) described our concern that the increasing rate of acute geopolitical crises — encapsulated in phrases like "great-power competition" — would tempt rivals to engage in increasingly risky cyber operations. Restraint, which might seem necessary in an initial crisis between rivals, could seem naïve in a second crisis and could be a dangerous sign of weakness in a third. Dangerous times call for dangerous measures and, in such times when both rivals' blood is up, decision-makers on either side cannot easily shrug off offensive cyber operations as a mere pressure release.

5 Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review* 3, no. 4 (Fall 2020): 30–53, http://dx.doi.org/10.26153/tsw/10962.

6 Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace 1986 to 2012* (Arlington, VA: Cyber Conflict Studies Association, 2013).

7 Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks*, Sept. 16, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/; and Benjamin Jensen and Brandon Valeriano, "What Do We Know About Cyber Escalation? Observations from Simulations and Surveys," Atlantic Council, November 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf.

8 David E. Sanger, Clifford Krauss, and Nicole Perlroth, "Cyberattack Forces a Shutdown of a Top U.S. Pipeline," *New York Times*, May 8, 2021, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html; and Ellen Nakashima, "Pressure Grows on Biden to Curb Ransomware Attacks," *Washington Post*, July 7, 2021, https://www.washingtonpost.com/national-security/ransomware-biden-russia/2021/07/06/ff52a9de-de72-11eb-b507-697762d090dd_story.html.

The final mechanism, Escalation Inversion, recognized our concern that if decision-makers think that war is likely, they may be tempted to use cyber capabilities early on to threaten, blind, or confuse their rival, especially if that rival is stronger. Since cyber capabilities could be used in a surprise attack to give an asymmetric advantage, a state might feel the need to attack first before its rival has a chance to do the same. As we wrote in these pages, "Cyber capabilities may be to World War III as mobilization timelines were to World War I," helping initiate a war that otherwise might have been avoided.

This rather long article (about 15,000 words) has already been split into two shorter pieces for easier digestion. These articles focus on three decades of intensifying cyber conflict,[9] a deeply disturbing trend that is often ignored in the cyber literature, and on the underestimated role of surprise in cyber attacks.[10] A third article, summarizing the four escalation mechanisms, is next up. Sadly, Bob will not be around to see it published.

At one of Bob's famous lunches with Columbia's political scientists — he would order, depending on whether we would walk north or south along Amsterdam Avenue, a gyro, steak sandwich, or thick Sicilian slice, always followed by him peeling a tiny Mandarin orange for his insatiable sweet tooth — we had the idea for our second paper.[11] The topic was how overclassification impacts cyber conflict and clouds the perceptions of both the attacker and defender. Bob was a longtime member (and former chair) of the CIA's Historical Review Panel, whose primary purpose is "to provide full and frank advice to the Director on declassification priorities," so classification issues were always on his mind.[12] This issue was closely tied to another of his most lasting contributions, which was on the perception and misperceptions of policymakers.

Our Columbia colleagues Tom Christensen and Keren Yarhi-Milo later paid tribute to Bob, who, they wrote, "focused on how leaders interpret the noisy world of international politics, showing persuasively that their cognitive biases, preexisting beliefs, and personal experiences often prove as consequential, or even more consequential, than objective conditions."[13] These factors could be substantially shaped by classification decisions. We concluded in our second collaboration that "[n]either the highest level of decision makers, nor their security apparatuses, have better than a murky and incomplete picture of cause and effect, which they spin for security, political, or bureaucratic advantage." The United States, in particular, classifies the punches it throws but shouts loudly about those it takes, clouding the relationship of cause and effect.

For Bob, who always had a special, abiding sympathy for decision-makers, this was less an accusation than a warning against self-deception and an admonition to keep a look out for one-sided perspectives and motivated reasoning.

## Influence and Inspiration

Many of Bob's cyber-related contributions were not in his actual written output, but in his influence in Washington, D.C. and among academics. He was often called down to the capital to share his perspective in the Pentagon, at the CIA, or at Fort Meade, the home of U.S. Cyber Command and the National Security Agency. His stature as a preeminent scholar of international relations meant that most of those in the room had read his work on "doubly dangerous" security dilemmas and misperceptions in graduate school or even as undergrads. When I raised the security dilemma in a meeting of the Defense Science Board Task Force on Cyber Deterrence, another member acknowledged automatically that we were "in Jervis territory."[14]

Bob's classic book *System Effects* profoundly influenced my 2019 article on persistent engagement,[15] one of the first articles to propose a causal argument and describe just what such engagement might mean in real terms. It also explored the ac-

9 Jason Healey and Robert Jervis, "How to Reverse Three Decades of Escalating Cyber Conflict," Atlantic Council, March 24, 2021, https://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-reverse-three-decades-of-escalating-cyber-conflict/.

10 Jason Healey, "Preparing for Inevitable Cyber Surprise," *War on the Rocks*, Jan. 12, 2022, https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/.

11 Jason Healey and Robert Jervis, "Overclassification and Its Impact on Cyber Conflict and Democracy," Modern War Institute, March 22, 2021, https://mwi.usma.edu/overclassification-and-its-impact-on-cyber-conflict-and-democracy/.

12 "Minutes 06/23/06," Public Interest Declassification Board, National Archives, accessed May 19, 2022, https://www.archives.gov/declassification/pidb/meetings/minutes06-23-06.html.

13 Thomas J. Christensen and Keren Yarhi-Milo, "The Human Factor: How Robert Jervis Reshaped Our Understanding of International Politics," *Foreign Affairs*, Jan. 7, 2022, https://www.foreignaffairs.com/articles/world/2022-01-07/human-factor.

14 *Final Report of the Defense Science Board Task Force of Cyber Deterrence*, Defense Science Board, Feb. 28, 2017, https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

15 Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton, NJ: Princeton University Press, 1997); and Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019), https://doi.org/10.1093/cybsec/tyz008.

ademic and military histories of the concepts of active defense and cyber deterrence. Earlier work of mine had covered similar ground looking at systemic cyber risk, though with less rigor than I could with Bob's input.

Generations of fellow academics will understand the deep satisfaction of being able to go to Bob's office (in the afternoon, of course, when he'd be reading a journal with his feet propped up) to talk through some new development. In this case, it was to explore how persistent engagement could be seen as a feedback loop, as he'd described in *System Effects*. The cyber optimists who saw persistent engagement as stabilizing were essentially arguing that defending forward with cyber operations would cause beneficial, negative feedback while we pessimists feared it would cause harmful, positive feedback and would spin out of control. Weeks later, I returned to excitedly reveal that — after I'd heard about an environmental scientist who had realized that climate change was driven by multiple, interacting feedback loops (winning a Nobel Prize in the process) — I'd realized that cyber conflict was not driven by *one* feedback loop but at least *eight*.

Bob's influence also helped Rose McDermott, his former student and long-time mentee,[16] to publish the first paper on the role of emotion in cyber conflict, in which she examined the "recent literature in psychology and neuroscience on the effects of emotion on both choice and action" in order to take a close look at "the influence of specific emotions on decision-making in cyber conflict."[17]

At Bob's intellectual home at the Saltzman Institute of War and Peace Studies, we are keeping his legacy alive. We are working to expand my paper with Bob on overclassification into a book chapter for the Modern War Institute. And, with my Saltzman colleagues Yarhi-Milo and Erica Borghard, we are exploring how cyberspace as a semi- or differently governed realm makes the role of political psychology particularly relevant, not least to understanding escalation and stability within cyber conflicts. Because cyber conflict is semi- or differently governed (not ungoverned), decision-makers are more likely to be impacted by uncertainty, leading them to rely more on traditional cognitive frameworks, heuristics, and emotions, which may be mismatched to the strategic environment or the expectations of rival states. Organizational cultures built to manage traditional conflicts (or fight traditional wars) may find themselves unsuited to cyber conflict while cognitive biases raise the risks of misperception and miscalculation. Bob was to share the role of principal investigator with others at Saltzman, but now we shall have to carry on without him.

My great sadness in working with Bob was a delay to the crowning paper of our Minerva-funded efforts: a 15,000-word, encyclopedic categorization of every dynamic of cyber conflict. It was essentially done in the autumn of 2020, when we first learned of Bob's diagnosis. But I just wanted to clear up one last detail before publication, clarifying under what conditions the offense or defense had the advantage in cyberspace. This was not just a simple blog post over the holiday break, as I'd hoped, but a year-long effort. The resulting paper is one I'm tremendously proud of, but the delay meant that we were unable to publish the work in his lifetime.

During the first half of summer break, I was blessed to have lunch almost every day with Bob and another legend, Dick Betts (gyro, Godfather hero,[18] or pepperoni roll). Because of the pandemic, that dropped to just the infrequent Zoom lunch with a group of colleagues from Saltzman and elsewhere. The gradually decreasing contact with Bob over the last two years means that I haven't quite accepted that he has passed. In a way, this thrills me and I'm unwilling to let it go, as it drives me to new ideas. But, even though he is gone, I know I will *always* be able to knock on his door again for more guidance, even if it is in my own imagination.

***Jason Healey*** *is a senior research scholar at Columbia University's School for International and Public Affairs, specializing in cyber conflict and risk. He started his career as a U.S. Air Force intelligence officer, helping create the world's first joint cyber command before moving to cyber response and policy jobs at the White House and Goldman Sachs. He was the editor of the first history of conflict in cyberspace,* A Fierce Domain: Cyber Conflict, 1986 to 2012. *He is on the DEF CON and Black Hat review boards and served on the Defense Science Board task force on cyber deterrence.*

16 Rose McDermott, "Robert Jervis: Scholarly Silverback," accessed at Saltzman Institute of War and Peace Studies, May 26, 2022, http://www.siwps.org/wp-content/uploads/diplo_McDermott_Jervis.pdf.

17 Rose McDermott, "Some Emotional Considerations in Cyber Conflict," *Journal of Cyber Policy* 4, no. 3 (2019): 309–25, https://doi.org/10.1080/23738871.2019.1701692.

18 "Godfather Combination Hero," Hamilton Deli, accessed May 19, 2022, https://menupages.com/hamilton-deli/1129-amsterdam-ave-new-york/menu-item?id=6142724.