The Eye of the Beholder and Subjective Escalation Theory

Abstract: Escalation can be framed objectively, as a ladder of actions in increasing order of intensity, or subjectively, as being in the "eye of the beholder." Building on the latter approach, we introduce subjective escalation as both a method and theory. The method examines changes to the judgments of apex policymakers to determine if there has been escalation from a baseline of strategic interaction to a new, more intense one. This method aligns with a primary reason to study escalation: to understand how apex policymakers will respond in future crises. Subjective escalation theory applies this to method to cyber conflict, based on the words and deeds of U.S. apex policymakers. Contrary to past literature, this approach reveals ample evidence of escalation, including that cyber operations helped drive one of the most important geopolitical shifts of the century, the U.S. switch from seeing China-as-partner to China-as-competitor.

Keywords: Political psychology, perception, escalation, cyber conflict, cyber operations, China, Russia, North Korea, United States

Part 1: Introduction and Problem

Escalation, in the view of structural theorists like Herman Kahn, occurs when the objective intensity or scope of competition ascends a ladder, the rings of which can be determined beforehand through rigorous, deductive analysis.[1] In contrast, Thomas Schelling and other perceptualists argued escalation is in the eye of the beholder, since thresholds "exist in the minds of the actors rather than in objective reality."[2] Conflict has escalated when "at least one party crosses what it, the adversary, or both parties perceive to be a critical threshold such that the nature of their strategic interaction has changed."[3]

We expand on the latter approach by introducing the *subjective escalation method* to examine changes to the perceptions, judgments, decisions and actions of apex policymakers over time.[4] Escalation has occurred if they judge adversary behavior has breached thresholds meaningful to them, moving from an initial strategic interaction to a new, more dangerous one. We then build on this method to develop the *subjective escalation theory of cyber conflict* to develop causal insights, using cyber operations as a worked example.

Subjectivity is not the same as arbitrary or irrational; asserting that escalation is in the eye of the beholder is not merely equating it to such famously partial topics like fashion, love, or beauty. Embracing subjectivity aligns methodology with a key reason to study escalation, to better predict in future crises whether policymakers will back down, simmer and plot, or punch back.

---

[1]Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Routledge, 2017).
[2]Forrest E. Morgan, Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, CA: RAND, 2008), p. 11.
[3]Erica D. Lonergan and Shawn W. Lonergan, *Escalation Dynamics in Cyberspace* (New York: Oxford University Press, 2023).
[4]The idea of "apex policymakers" is explored below, but in the United States includes the president and those roughly three levels below.

Ironically, this can also be a more repeatable methodology than objective approaches, which have no obvious way to decide between empirics. A minor border incursion of three battalions is surely more of an escalation than just using two, but is either worse than deploying a treaty-breaking strategic weapon or blinding a surveillance satellite? Academics placing one on a higher rung than another prioritize their own subjective assessments over those of policymakers. Nor are there objective ways to disentangle the message a state intended and the one that their rival believed.[5]

Understanding subjective perceptions is especially useful for understanding escalation in diplomatic maneuvering, grey-zone operations, espionage, and cyberspace. These kinds of competition rarely lead to deaths and have few "objects" about which to be objective. In cyber competition, the weapons and targets are, after all, mostly just ones and zeroes. Since little can be objectively determined, assessments about escalation become matters of perception and judgment. This method simply preferences the judgments of policymakers.

Focusing on the breaking points of policymakers removes these dilemmas: the escalation of any incident depends on how much policymakers care afterwards. And past findings from political psychology suggest that vivid incidents drive policymakers more than objective measures and they take more risks when they are angry[6] and believe they are losing.[7]

This article will conduct a deep analysis of cyber conflict, as there is a mismatch between scholarship and the perception of policymakers.

Part 1.1. Puzzling Gap Between Policymakers and Scholarship

[5]Robert Jervis, *Perception and Misperception in International Relations*, new ed. (Princeton, NJ: Princeton University Press, 2017), p. 205.
[6]Rose McDermott, "Emotional Dynamics of Cyber Conflict," *Journal of Cyber Policy* 4, no. 3 (2019): 309–325.
[7]Keren Yarhi-Milo, "In the Eye of the Beholder: How Leaders and Intelligence Communities Assess the Intentions of Adversaries," *International Security* 38, no. 1 (2013): 7–51.

Substantial international relations scholarship has concluded that "cyber operations have not led to escalation, either in cyberspace or through the use of other instruments of power. Rather … the interactions have been largely limited to tit-for-tat, proportionate responses across cyber and non cyber capabilities."[8] Rivals have been "surprisingly tolerant"[9] of cyber operations which offer "bargaining benefits,"[10] conciliatory signaling, and a strategic off-ramp during crises.[11]

But such soothing assessments, however well founded, are at odds with U.S. policymakers' stormy responses to cyber operations, such as Chinese cyber espionage. Detected in the early 2000s, these operations were indeed initially shrugged off. Eager to engage China as a partner, president George W. Bush never meaningfully complained to China nor, initially, did president Barack Obama. During a 2009 appearance with Chinese president Hu Jintao, Obama avoided discussing cyber, compared to eight mentions of "mutual cooperation" on energy, the environment, and the economy.[12]

But the United States decisively shifted from any tolerance during an extraordinary and overlooked Beijing meeting on May 4 and 5, 2012. Deputy secretary of state William Burns, joined by undersecretary of defense for policy James Miller and *de facto* cyber ambassador Chris Painter, raised specific cyber allegations with China's vice foreign minister and the deputy commander of the People's Liberation Army.[13] Enough, the Americans pronounced, was enough. Within ten

[8]Lonergan and Lonergan, *Escalation Dynamics in Cyberspace*, p. 131.
[9]Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks*, September 16, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.
[10]Brandon G. Valeriano and Ben Jensen, "The Myth of the Cyber Offense: The Case for Cyber Restraint," Cato Institute Policy Analysis No. 862 (2019), p. 4.
[11]Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics," *Journal of Cybersecurity* 5, no. 1 (2019): tyz007; Lonergan and Lonergan, *Escalation Dynamics in Cyberspace*.
[12]Kevin Hechtkopf, "Text: Obama's Speech on U.S.-China Relations," *CBS News*, July 27, 2009, https://www.cbsnews.com/news/text-obamas-speech-on-us-china-relations/.
[13]Author interview with Chris Painter, former cyber coordinator, U.S. Department of State, February 19, 2026.

months, the spat was public, with Tom Donilon, Obama's national security advisor, railing about how the "unprecedented scale" of China's intolerable espionage had upended any budding partnership:

> From the President on down, this has become a key point of concern and discussion with China at all levels of our governments. [The United States needs from China] a recognition of the urgency and scope of this problem and the risk it poses … to our overall relations.[14]

In June 2013, Obama – again standing next to a Chinese president, this time Xi Jinping – no longer purred about mutual cooperation but rather channeled his "deep concerns … around [China's] theft of intellectual property [and] hacking into … our financial systems, our critical infrastructure."[15] Obama's cyber coordinator, Michael Daniel, recalled that "we decided to make it explicit that if the Chinese wanted to get something in other areas, then we had to make progress," so that "eventually, every high-level engagement with the Chinese involved bringing up intellectual property theft, including at the Presidential level."[16]

Cyber operations provided no bargaining benefits to China. They were not conciliatory signaling, offering a de-escalatory offramp, or mitigating a geopolitical crisis. Cyber operations helped create the rupture, escalating from a side show to center stage for the most powerful policymaker in the world, the U.S. president, in his relationship with America's sole rival. The president had other complaints as well, such as human rights and China's claims in the South China Sea. But such

[14]White House, "Remarks by Tom Donilon, National Security Advisor to the President: 'The United States and the Asia-Pacific in 2013,'" March 11, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisor-president-united-states-an.
[15]White House, "Remarks by President Obama and President Xi Jinping of the People's Republic of China after Bilateral Meeting," June 8, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-
[16]Michael Daniel (Obama cyber coordinator) and Chris Painter, email to Healey, September 10, 2024.

grievances ranked far behind those about cyber behavior, which marked the first major shift from China-as-partner to China-as-rival, perhaps the most seismic diplomatic event of the century.

Presidents Donald Trump and Joseph Biden extended and expanded Obama's policies, each taking unprecedented new steps, institutionalizing vastly larger cyber commands conducting more aggressive campaigns under more permissive authorities. While there was no resort to use of armed attack, their responses locked in cyber competition at objectively higher levels. In contrast to prior findings by Keren Yarhi-Milo that subjective threat perception of policymakers diverged from that of the more objective intelligence professionals, in cyber, these groups are broadly aligned.[17]

These responses highlight the two ways this paper advances understanding of political psychology, by reframing assessments of escalation in terms of perception of apex policymakers and how their responses are often driven by psychological factors. Indeed, much of the U.S. strategy of engaging persistently in cyberspace to impose costs on adversaries could be explained as the response to operating in a domain of loss.

Part 1.3. Structure of this Article

This paper proceeds in several parts. Part 2 compares the existing method- and theory-forward approaches with subjective escalation theory while Part 3 both describes how words and deeds can act as proxies to understand perception and sets out the baseline strategic interaction. Part 4 examines the words and deeds of U.S policymakers to look for perception of escalation to a more intense strategic cyber interaction, complemented by case studies of North Korea, China, and Russia in Part 5. Part 6 includes analysis, including possible psychological mechanisms, and recommendations.

[17]Yarhi-Milo, "In the Eye of the Beholder."

The core of this article are the 20+ lines of evidence in Part 2, spanning words and deeds, almost every one of which shows a shift to a more intense strategic interaction after 2012. Cyberspace reeks of escalation. Unlike policymakers' concern over terrorism or nuclear war, their perception of cyber operations has never reverted to the mean; it consistently rises with decreases only over short periods, if ever. Because of pressure on the perception of apex policymakers, there will likely be a persistent, nearly inexorable rise of tensions in cyberspace which might be moderated but is likely to prove difficult to escape.

Part 2: Explaining Cyber Escalation

Escalation is the "the expansion or intensification of conflict," which "the relaxation or erosion of limits on the use of force that are recognized, either formally or informally, by one or more of the combatants."[18] Such escalation could be "employing types of weapons not previously used in the conflict or attacking new categories of targets [or] expanding the geographic scope of a conflict," respectively called vertical escalation and horizontal escalation.[19]

To explore cyber escalation, the theory of subjective cyber escalation competes with two other approaches. Broadly, one is more method-forward, relying on *ex-ante* determination of meaningful thresholds. The other approach is more theory-forward, exploring why cyber competition has not and perhaps never will escalate.

Method-Forward Approaches

The method-based approach is led by scholars like Brandon Valeriano, et al; Erica Lonergan and Shawn Lonergan; and Sarah Kreps and Jacqueline Schneider, who use case studies, exercises,

[18]Morgan et al., *Dangerous Thresholds*, p. 14.
[19]Ibid., p. 18.

surveys, and large-n data sets to assess whether a particular cyber incident crossed some ex-ante threshold.[20] Many rely on a mechanism we call *bilateral-counteraction*: after being on the receiving end of a cyber incident, does the target "respond with more intense and costly cyber means (cyber escalation within the cyber domain) or through breaching the cyber-kinetic threshold (cross-domain escalation)."[21] Because there are few objectively measurable inputs, the escalation is based on the spiciness of any response.

Assessments based on bilateral-counteraction methods have concluded that "[c]yber operations have not led to escalation, either in cyberspace or through the use of other instruments of power. Rather … the interactions have been largely limited to tit-for-tat, proportionate responses across cyber and non-cyber capabilities."[22] Cyber operations instead create "bargaining benefits and crisis offramps,"[23] provide "accommodative signaling,"[24] and "provide a non-kinetic option for leaders who feel pressure to act in a crisis."[25] A "Las Vegas effect" ensures what happens in cyberspace, stays in cyberspace.[26]

If rivals indeed show restraint, then intensity of cyber stimuli would remain at the long-term mean or soon revert to it with no change in strategic interaction, with patterns like those in the simplified curves of Figure 1.[27]

---

[20]See Lonergan and Lonergan, Escalation Dynamics in Cyberspace; Kreps and Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains"; and Brandon Valeriano and Ryan C. Maness, Cyber War versus Cyber Realities: Cyber Conflict in the International System (Oxford: Oxford University Press, 2015).
[21]Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly* 13, no. 3 (2019): 122–145.
[22]Lonergan and Lonergan, *Escalation Dynamics in Cyberspace*, p. 131.
[23]Valeriano and Jensen, "The Myth of the Cyber Offense," p. 4.
[24]Lonergan and Lonergan, *Escalation Dynamics in Cyberspace*.
[25]Rovner, "Cyber War as an Intelligence Contest."
[26]Valeriano and Maness, Cyber War versus Cyber Realities. p.153
[27]See Jason Healey, "Measuring Policy Effectiveness of Cyber Defensibility and Deterrence," *Lawfare*, November 16, 2019, https://www.lawfaremedia.org/article/measuring-policy-effectiveness-of-cyber-defensibility-and-deterrence.

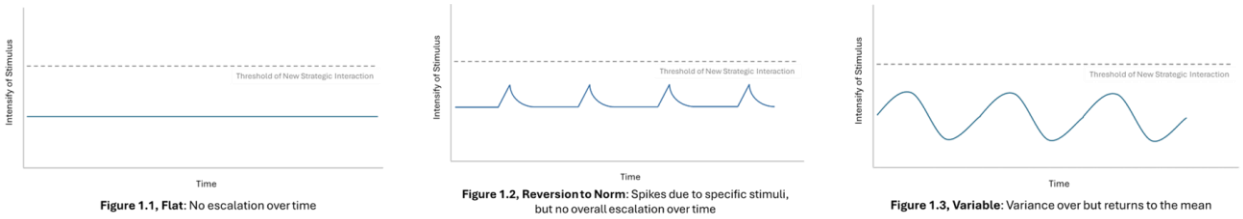


Figure 1.1, Flat: No escalation over time

Figure 1.2, Reversion to Norm: Spikes due to specific stimuli, but no overall escalation over time

Figure 1.3, Variable: Variance over but returns to the mean

Figure 1: Patterns of Intensity Over Time Showing No Escalation

In the unlikely situation there was absolutely zero variation, the curve would be a flat line as in Figure 1.1, never approaching the threshold of a new strategic interaction. Intensity would more realistically follow a saw-tooth pattern, as in Figure 1.2 (perhaps if concerns spike after particularly severe incidents) or a cycle, with words and deeds varying over time, but staying close to the long-term mean, as in Figure 1.3 (if perceptions are modulated by exogenous factors like a new administration or geopolitical crises).

Theory-Forward Approaches

The second approach often relies on the findings from the method-forward approach to drive theoretical explanations, which fall into two categories. First are what we group as cyber-information theories, which anchor on cyber operations being based on information, not traditional force. Accordingly, theories like cyber subversion,[28] secret statecraft,[29] and cyber as an intelligence contest,[30] are largely unconcerned about escalation of cyber competition. By itself in a second category, cyber persistence theory acknowledges that cyber competition has gotten substantially worse but is relatively unbothered about escalation.

[28]Lennart Maschmeyer, *Subversion: From Covert Operations to Cyber Conflict* (New York: Oxford University Press, 2024).
[29]Jon R. Lindsay, *Age of Deception: Cybersecurity as Secret Statecraft* (Ithaca, NY: Cornell University Press, 2025).
[30]Rovner, "Cyber War as an Intelligence Contest."

Despite key distinctions, these theories view cyber operations largely as a competition of information, typically not meant to coerce or shift the military balance. So, they should be less likely to escalate than military operations and indeed victims were assessed as being "surprisingly tolerant of cyber operations."[31]

Like the method-forward approach, the curve of these arguments should show no lasting increase in strategic interaction over time, as in Figure 1. If cyber is an intelligence contest, for example, the curve should vary cyclically like Figure 1.3. Confronted by audacious attacks, a new administration would respond assertively, then return to status quo ante as they gain "a basic understanding of how things work and what limitations exist."[32]

Cyber persistence theory acknowledges that cyber operations have gotten more intense over time but can be unconcerned about the dangers. Nation-state cyber campaigns are "deliberately calibrated to remain below a threshold that would likely elicit an armed response, seeking instead to produce cumulative gains over time."[33] Such constant contact of rival's cyber forces matures their agreed competition, the only path to stability and reliable red lies. The safest path for all states is to accordingly eschew restraints and engage persistently against rivals.[34]

The expected curve then for cyber persistence theory would be an initial rise in the earlier phases of constant contact, as in Figure 2.2, which then declines as tacit bargaining matures and intensity decreases over time.

[31]James Shires, Robert Chesney, and Max Smeets, *Cyberspace and Instability* (Edinburgh: Edinburgh University Press, 2023).
[32]Valeriano and Maness, Cyber War versus Cyber Realities.
[33]Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (New York: Oxford University Press, 2022), p. 7.
[34]Fischerkeller et al., *Cyber Persistence Theory*, p. 87.

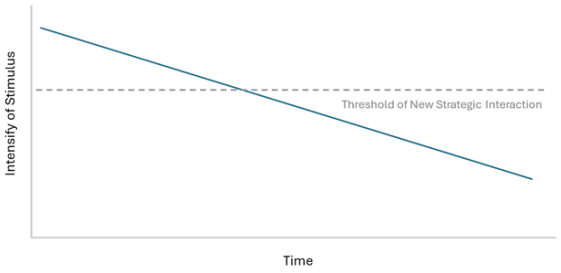


Figure 2.1, Decrease: De-escalation over time.

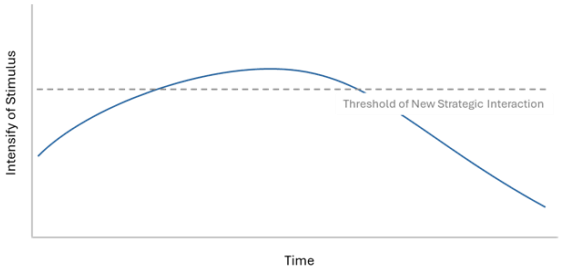


Figure 2.2, Rise and Fall: Early escalation but longer-term decrease

Figure 2: Patterns of Intensity Over Time Showing De-Escalation

None of the method- or theory-forward approaches would predict an incline to the curve of intensity, such as in Figure 3. Any evidence of such an incline over time would suggest these theories are a poor fit to the data.

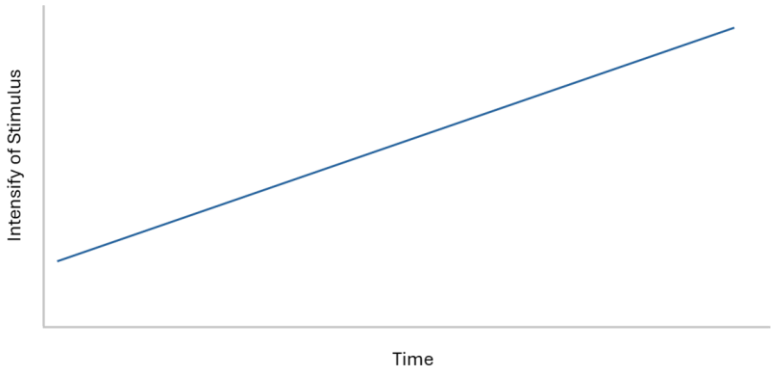


Figure 3, Incline: Pattern of intensity over time showing escalation

The Subjective Escalation Approach

The final approach, the subjective escalation approach, complements the others, proceeding from the insight that escalation is the *perception* of breached thresholds leading to a "significant qualitative change in the conflict"[35] and a new strategic interaction.[36] Apex policymakers are

[35]Morgan et al., *Dangerous Thresholds*, p. 8.
[36]Lonergan and Lonergan, *Escalation Dynamics in Cyberspace*.

humans and, like all humans, are affected by emotional responses and cognitive biases which must be incorporated in international relations analysis.[37]

Escalation, accordingly, can also be determined not by prior, rational assessments but by the interpretations of apex policymakers themselves, the ultimate arbiters of choices over war and peace. The core of this method is to compare a baseline strategic interaction with a future period of strategic interaction, to see the impact of any intervening stiumli. Subjective methods are particularly useful for any kind of competition with few quantifiable objects or which is fought largely hidden from view, such as diplomatic maneuvering, grey-zone operations, espionage, and cyber conflict.

Even well afterwards, it can be hard to pin down even the most basic facts, such as the attacker's intent, the amount of effort or force involved, or the overall impact. Any assessments of escalation come down to questions of judgment. The subjective method simply elevates the judgment of apex policymakers over those of academics.

The figures below show a simple binary comparison of the intensity of perceptions, based on the earlier figures. Escalation has occurred if policymakers believe adversaries have crossed thresholds creating a new strategic interaction that is meaningfully "worse" than the baseline, as in Figure 4.3 and de-escalation if things are "better" (4.2).

[37]Jervis, *Perception and Misperception in International Relations*.

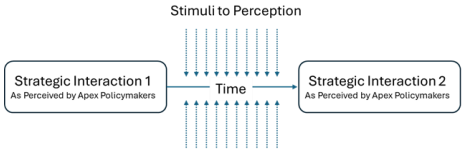


Figure 4.1: Tracking Subjective Perception of Escalation
No Change Over Time; Similar Intensity Between Strategic Interactions

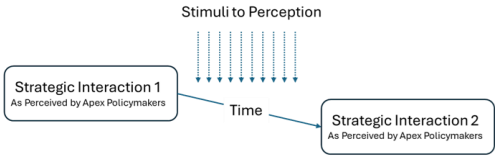


Figure 4.2: Perception of De-Escalation, Decreasing Over Time to Less-Intense Strategic Interaction

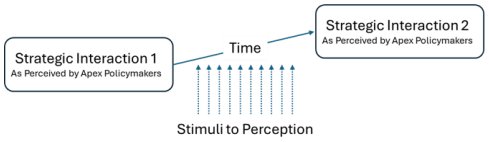


Figure 4.3: Perception of Escalation, Increasing Over Time to More-Intense Strategic Interaction

Figure 4.1 to 4.3: Subjective Escalation Comparing Different Relationships of Strategic Interactions Over Time

As time continues, there can be further shifts, such as higher-then-lower (4.4) or higher-and-higher (4.5).

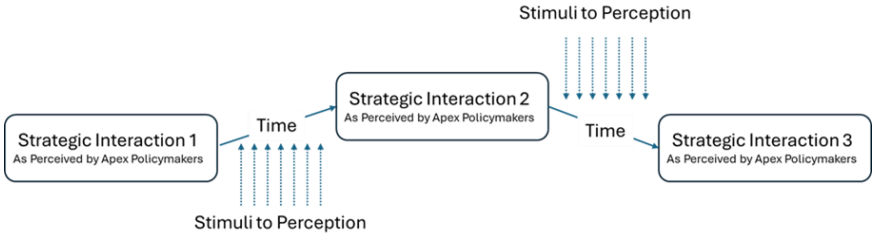


Figure 4.4: Perception of Escalation then De-Escalation, Returning to Status Quo

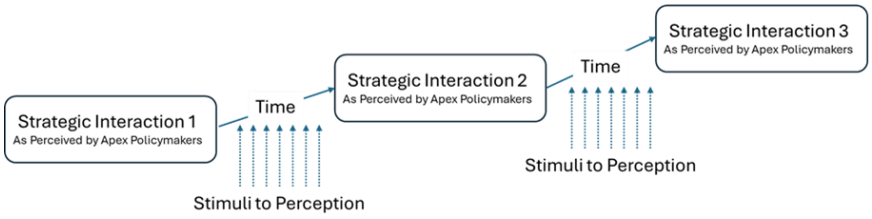


Figure 4.5: Perception of Escalation to Two New Interactions

As "worse" can mean different things to different policymakers (e.g., more dangerous or disrespectful, ignoring prior agreements), they need only agree that the situation has meaningfully

deteriorated. Moreover, any stimuli which shifts perceptions must be included in the analysis; it is not necessary to have a one-to-one match between stimuli and responses.

If policymakers respond, those serve as additional confirmation of the new reality, which may be in turn interpreted by rival policymakers as escalation, leading to security-dilemma dynamics. This is especially true for **intensifiers**, responses which objectively deepen the underlying competition, perhaps by relaxing prior restraints or committing more military forces.

Policymakers will experience the transition between to a more intense strategic interaction as a chaotic, confusing phase change: nothing is routine anymore as everything feels unprecedented. Their old mindsets and methods will be mismatched to the new reality, evidenced by reports of being in “unchartered territory” as they “struggled to respond." They will call out adversary behavior as “reckless,” “brazen,” “aggressive,” or a “gamechanger” or “wakeup call.” All are presumptive evidence of crossed thresholds.

The transition is a time of **norm turbulence**. Believing adversaries are seeking revisions to the status quo, policymakers demand new norms to determine the “rules of the road.” Once policymakers adapt to the new strategic interaction, such calls diminish as they adapt and approve responses which had been previously unthinkable. Responses may snowball, quickly covering an unprecedently wide range of available levers of power.

Subjective Escalation Theory for Cyber: Specifically applied to cyber competition, this paper uses the words and deeds of U.S. apex policymakers to establish the baseline of strategic interaction and as proxies for their perception about the stimuli, generally malicious cyber incidents.

As Jonathan Mercer argued, subjective and objective (or psychological and rational) approaches have strengths but neither "has a lock" on being the right correct. In particular, "subjective models can highlight the weakness of objective accounts."[38]

Subjective escalation theory aligns perception-based definitions of escalation with perception-based evidence. It expands the existing literature by permitting – even mandating – analysis of the cumulative effects of repeated interactions over time across a broader range of evidence than permissible in the objective approaches. It also can capture when apex policymakers perceive escalation but choose delay (which may make the response seem unconnected to the stimulus) or inaction (which might be mistaken for insouciance). For example, U.S. leaders responded modestly to Russia's 2016 interference in U.S. elections, mistakenly believing they could delay until the next, Democratic administration.[39] Policymakers may also delay or choose inaction in the face of escalation because of domestic or international pressures, a lack of ready capabilities, or fear that action will lead to even further escalation. All would be missed in assessments of bilateral counteraction but not subjective escalation.

Moreover, subjectivity can sneak into ostensibly objective methods, as researchers must use their own informed-yet-still-subjective judgement on coding the intensity of incidents in a large-n dataset, deciding if some categories of incidents are out-of-scope, determining who counts as "elite," and assessing about whether a particular response should count as tit-for-tat or escalation. The interpretations of policymakers are more directly relevant and no more subjective.

[38]Jonathan Mercer, "Rationality and Psychology in International Politics," *International Organization* 59, no. 1 (2005): 77–106.
[39]David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2019).

Lastly, subjective escalation taps into insights from political psychology. Keren Yarhi-Milo, for example, summarized that policymakers' perceptions of adversary intentions are influenced by information "that is vivid, personalized, and emotionally involving" and "reluctant to rely on evidence that is abstract, colorless, objective, or less tangible." Further, apex policymakers, facing losses from constant cyber incidents, may be angry and operating in a domain of loss, willing to take more risky gambles.[40] Fear leads people to be more risk averse, while anger causes the opposite.[41]

This unfortunately leads to a dark prediction: that states will find themselves in a spiral of cyber conflict from which they will find it very difficult to exit. Apex policymakers of rival states will be constantly tested with a fresh set of vivid incidents over time across an expanding set of targets. It will be very hard to come to agreement with rivals about unacceptable behavior because the salience of incidents against the same target will change over time, salience will differ between individual policymakers, and policy makers are swapping in and out all the time (especially in democratic countries).

As the following material may be unfamiliar to non-cyber specialists, Table 1 below highlights the incidents cited by apex policymakers. Most are included because of policymaker responses reflected in the public record; several others only emerged though interviews.

[40]Jack S. Levy, "Prospect Theory, Rational Choice, and International Relations," *International Studies Quarterly* 41, no. 1 (1997): 87–112.
[41]As summarized in McDermott, "Emotional Dynamics of Cyber Conflict."

Table 1: Dataset of Incidents Driving Words and Deeds of U.S. Apex Policymakers					
Count	**Short Name of Incident or Actor**	**Date**	**Actor**	**Reported Purpose or Impact**	**Description**
1	Morris Worm	1988	Non-state (individual)	Disruption	Major disruption disrupting ~10 percent of the early Internet
2	Solar Sunrise	1998	Non-state (teenagers)	Disruption[42]	Intrusions into US military sites, suspected of being Iraqi attack
3	Moonlight Maze	1999-2005?	Russia	Espionage/Theft of Information	Large-scale, persistent espionage targeting US military and related targets
4	Mafiaboy attacks	2000	Non-state (individual teenager)	Disruption	Distributed denial of service (DDoS) against e-commerce sites
5	Code Red	2001	Unknown, likely non-state	Disruption	Worm which disrupted substantial portion of global Internet
6	Nimda	2001	Unknown, likely non-state	Disruption	Worm which disrupted substantial portion of global Internet
7	Chinese Theft of Intellectual Property	2000s+	China	Espionage/Theft of Information	Long-term campaign to steal IP, mostly but entirely through cyber means
8	Estonia	2007	Non-state (Russian-linked hactivists)	Disruption	Major, long-term DDoS disrupting the entire nation
9	Buckshot Yankee	2008	Russia	Espionage/Theft of Information	Espionage into classified US military networks
10	Georgia	2008	Non-state (Russian-linked)	Disruption	Large-scale DDoS coinciding with Russian invasion of Georgia

[42]The military concern, which led to the deputy secretary briefing the president, was that the incident might have been the beginning of a disruptive attack. This was mistaken, but included here as that belief drove the response.

11	Conficker	2009	Unknown	Unknown	Large-scale botnet for unknown purpose
12	Aurora	2010	China	Espionage/Theft of Information	Large-scale espionage targeting Google and other tech companies
13	RSA Security	2011	China	Espionage/Theft of Information	Advanced operation to steal encryption tech to further espionage
14	Ababil	2012	Iran	Disruption	Long-term attempted disruption of US financial institutions
15	Shamoon	2012	Iran	Disruption	Large scale disruption of Saudi Aramco and Qatari Rasgas
16	Target	2013	Non-state	Espionage/Theft of Information	Criminal theft of credit card data from retailer
17	Sony Pictures Entertainment	2014	North Korea	Disruption	Intrusion, disruption, and release of stolen information
18	OPM	2015	China	Espionage/Theft of Information	Espionage stealing personnel records of almost all US government employees
19	Bank of Bangladesh	2016	North Korea	Espionage/Theft of Information	Attempted theft of $1 billion through SWIFT payment network
20	Election Interference	2016	Russia	Espionage/Theft of Information	Espionage and release of stolen information to interfere with presidential election
21	WannaCry	2017	North Korea	Disruption	Major global disruption
22	NotPetya	2017	Russia	Disruption	Major global disruption, initially targeted at Ukraine
23	Colonial Pipelines	2020	Non-state (Russian-linked ransomware gangs)	Disruption	Ransomware disruption of US pipeline, disrupting energy distribution to entire East Coast
24	SolarWinds	2021	Russia	Espionage/Theft of Information	Large-scale, sophisticated espionage affecting 100+ targets

25	Hafnium (Microsoft Explorer)	2021	China	Espionage/Theft of Information	Threat actor behind large-scale espionage campaign, turned to indiscriminate mass exploitation
26	JBS	2021	Non-state (Russian-linked ransomware gangs)	Disruption	Disruption of the world's largest meat producer
27	Grain Co-ops	2021	Non-state (Russian-linked ransomware gangs)	Disruption	Disruption of grain cooperatives by ransomware
28	ICBC US	2023	Non-state (Russian-linked ransomware gangs)	Disruption	Disruption of Chinese bank, affecting crucial US Treasuries market
29	Change Healthcare	2024	Non-state (Russian-linked ransomware gangs)	Disruption	Ransomware disruption which disrupted US healthcare system
30	Volt Typhoon	~2021-	China	Disruption	Threat actor prepositioned to cause disruption in US infrastructure
31	Salt Typhoon	~2020-	China	Espionage/Theft of Information	Threat actor conducting widespread espionage into U.S. and other nation's telecommunications

Part 3: Words and Deeds as Proxies for Perception. This section explains the framework of words and deeds to track perception of cyber escalation.

Words: If policymakers perceived there had been no escalation, then over time their speeches and policies would discuss cyber in general terms with only potential future impact, such as generic "cyber doom" scenarios (like cyber Pearl Harbors).[43] There will be little variance over time, as in Figure 4.1, with any increases in perceived intensity subsequently returning to the mean. If policymakers do perceive escalation, their speeches and strategies will use vivid language, per Figure 4.3, calling out specific adversary behavior. If there is de-escalation, per Figure 4.2, they will stop calling out specific behaviors or issuing cyber policies in response.

Deeds: If policymakers did not believe there had been meaningful escalation, then their responses today would be similar to those of the past, with no change to strategic interaction. Conversely, there is evidence of escalation if actions over time have become more substantial, more frequent, or both. Deeds are stronger proxies of perception than words and include emergency meetings of national security policymakers, sanctions and indictments, or creation of new organizations. As with words, such proxies can also indicate de-escalation, such as if policymakers pare back budgets, cyber-related commands, and operations.

Plausibility Probe: To test whether this method is a reasonable proxy for policymaker's perception over time, we conducted a simple comparison of frequency of select terms in the

[43]Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology & Politics* 10, no. 1 (2013): 86–103.

National Security Strategy (NSS)[44] and mentions in presidential documents, by year.[45] As shown in Figures 5.1 and 5.2, the mentions vary based on the intensity of policymaker concern. In the 1980s, nuclear weapons were the top concern, though this shifted to terrorism especially after 2001.

While this probe is just for the plausibility of the method, it is worth noting that by the mid-2010s, cyber is mentioned in the NSS more than nuclear weapons and terrorism combined and by the Biden administration, cyber is mentioned three times more than nuclear. While the mentions of nuclear weapons and terrorism in both datasets varied over time, the total documents mentioning cyber grew consistently over the entire period.

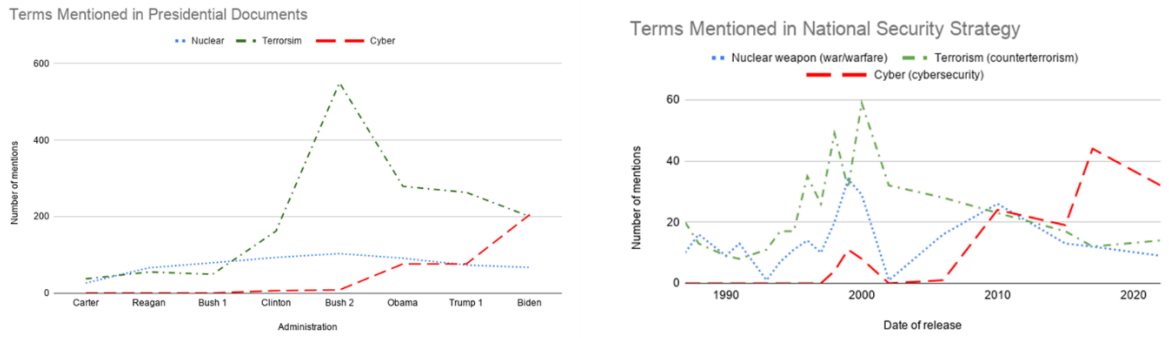


Figure 5: Mentions of Key Terms in NSS (left, by year of issuance) and Presidential Documents (right, by administration)

[44]Downloaded from the Office of the Secretary of Defense Historical Office, "National Security Strategy," https://history.defense.gov/Historical-Sources/National-Security-Strategy/. Each document was searched using terms related to nuclear weapons or war (excluding waste or energy), terrorism or counterterrorism, and cyber or cybersecurity.

[45]Document mentions were from a search of the University of California, Santa Barbara, *The American Presidency Project*, https://www.presidency.ucsb.edu/advanced-search (accessed March 12, 2026). Each presidential administration was searched using the same terms as for the NSS.

Part 3.1: Initial Strategic Baseline

The first step in investigating subjective escalation is to establish perceptions of apex policymakers in the baseline period, in this case from the late 1990s to 2012. Within this period, responses looked like those in Figure 1, with no clear escalation over more than 15 years. While they frequently interpreted incidents as crossing important thresholds, we assess their responses did not constitute a "significant qualitative change."

In speeches in 1998 and 2000, Clinton worried generally that "adversaries may attempt cyberattacks against our critical military systems and our economic base."[46] He convened a major summit at the White House in 2000[47] (in response to major attacks by a teenager, nicknamed mafiaboy) and called out two major worm outbreaks (NIMDA and Code Red) in the 2003 national cyber strategy,[48] incidents which the Richard Clarke, the special assistant to the president for cyber issues, earlier highlighted in rare congressional testimony.[49] Obama in 2009 worried about the U.S. "disorganized" approach in response to the Conficker worm.[50] Despite such concerns, Obama wrote in a 2010 op-ed that, "[s]o far, no one has managed to seriously damage or disrupt our critical infrastructure networks."[51]

---

[46]White House, "Remarks by the President at the United States Naval Academy Commencement," May 22, 1998, https://clintonwhitehouse4.archives.gov/WH/New/html/19980522-4986.html; William J. Clinton, "Commencement Address at the United States Coast Guard Academy in New London, Connecticut," May 17, 2000, https://www.presidency.ucsb.edu/documents/commencement-address-the-united-states-coast-guard-academy-new-london-connecticut-0

[47]C-SPAN, "Special White House Briefing on Internet Security," February 15, 2000, https://www.c-span.org/program/white-house-event/internet-security/98752

[48]White House, "National Strategy to Secure Cyberspace," 2003, https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

[49]Richard Clarke, "Computer and Online Security" (testimony to Senate Judiciary Committee, C-SPAN, February 13, 2002), https://www.c-span.org/program/senate-committee/computer-and-online-security/110030.

[50]White House, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009, https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure/

[51]The American Presidency Project, "Op-ed by President Obama: Taking the Cyberattack Threat Seriously," July 19, 2012, https://www.presidency.ucsb.edu/documents/op-ed-president-obama-taking-the-cyberattack-threat-seriously

A comparison of national cyber strategies and key documents from the administrations of Ronald Reagan,[52] Clinton,[53] and Bush[54] show no major change in language, using similar modal verbs to say that adversaries "may" attack in future and vulnerabilities "could be" exploited by them. Major announcements and strategies followed a similar pattern, nor is there any record of senior U.S. officials meaningfully complaining about cyber incidents to their counterparts in China, Russia, or elsewhere. Presidents and secretaries of state fretted over the rules of the road, exemplified by Obama's International Strategy for Cyberspace, in which norms were mentioned 25 times.[55] Press statements from the high-level U.S.-China Strategic and Economic Dialogue focused on building bridges, not airing cyber grievances.[56]

These calm words corresponded with restrained deeds. Between 2003 to 2005, not a single incident needed substantial reaction by the White House such as a convening of the Deputies Committee of the NSC,[57] nor had policymakers declared any cyber-related state of emergency. Cyber was important enough so that the number of policy-related directors at the White House boomed from about five in 2003 to perhaps twenty later that decade, with the creation of a dedicated cyber directorate at the NSC.[58] But the number went no higher until the 2020s.

While there were many "wake-up calls," these did not obviously lead to a new strategic interaction. In March 1998, deputy secretary of defense John Hamre briefed Congress on Solar Sunrise, an

[52]White House, "National Policy on Telecommunications and Automated Information Systems Security," September 17, 1984, https://irp.fas.org/offdocs/nsdd145.htm
[53]White House, "National Plan for Information Systems Protection, Version 1.0," January 1, 2000, https://irp.fas.org/offdocs/pdd/CIP-plan.pdf
[54]White House, "The National Strategy to Secure Cyberspace," February 2003, https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf
[55]White House, "The International Strategy for Cyberspace," May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf
[56]Department of State, "Remarks at U.S.-China Strategic and Economic Dialogue Opening Session," May 3, 2012, https://2009-2017.state.gov/secretary/20092013clinton/rm/2012/05/189213.htm
[57]Author discussion with Greg Rattray, a policy director in the National Security Council, October 10, 2025.
[58]Author discussion with Chris Painter, March 31, 2026.

intrusion into the Department of Defense (DoD), which was "widespread, systematic and [possibly] preparation for a coordinated attack" by Iraq. (It was actually just a few teenagers.) Soon after, Hamre briefed Congress on Russia's Moonlight Maze espionage campaign, which was "a real wake-up call for us … a foreign power that broke into our systems and simply wouldn't leave."[59] Obama made perhaps the first major presidential speech on cyber in 2009, mentioning intrusions into his own election campaign, the 2008 Buckshot Yankee intrusion against classified military systems, and how Russian "cyber attacks crippled Georgian government websites" during their 2008 invasion.[60] Deputy defense secretary William Lynn wrote in a major 2010 article that the Pentagon treated Buckshot Yankee intrusion as a "turning point in U.S. cyberdefense strategy."[61] Secretary of State Hillary Clinton in 2010 called on China to investigate Google's claims that it had been behind a massive espionage campaign, dubbed Aurora.[62]

These incidents helped drive important changes, such as Buckshot Yankee helping drive creation of U.S. Cyber Command, with roughly 1000 personnel. Still, there was not clearly a new strategic interaction as the U.S. military maintained "an approach of restraint" and a "doctrine of 'minimal use' of cyberweaponry against other states," according to one defense secretary.[63] As a later Pentagon chief of staff said of this period, "I can count on one hand, literally, the number of offensive operations that we did at the Department of Defense."[64]

Part 4: Cyber Escalation as Reflected in Words and Deeds

[59]Sanger, *The Perfect Weapon*, p. 13.
[60]White House, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009, https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure
[61]William F. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September 1, 2010, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain?check_logged_in=1
[62]Hillary Rodham Clinton, Secretary of State, "Remarks on Internet Freedom," Department of State, January 21, 2010, https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm
[63]"Retirement Ceremony for General Keith Alexander," The Free Library, accessed February 24, 2026, https://www.thefreelibrary.com/Retirement+ceremony+for+General+Keith+Alexander.-a0367545474.
[64]Sanger, *The Perfect Weapon*.

After that baseline period, from 2012 onwards, apex policymakers used their speeches and key documents to declare a new, clearly more intense strategic interaction.

Part 4.1. Escalation as Reflected in Words

Interactions Between Heads of Government. By 2013 policymaker's words showed a marked change from the initial baseline, with Obama raising his "deep concerns" to Xi in front of journalists during their 2013 summit,[65] and personally reiterating the message in St. Petersburg (2013) and The Hague (2014).[66]

Chris Painter, America's top cyber diplomat at the time, remembers that "Obama said that this issue was important enough that we were willing to have friction in the larger bilateral relationship— elevating this from a mere cyber issue." There was sustained messaging "in literally every meeting with them," at the Cabinet level. Painter suspects that if the president "neglected to keep saying it [the Chinese] would have said 'ok, they're over it' and move on."[67]

Presidential words against Russia were equally severe. Obama raised the 2016 election interference with Putin several times, explaining later that "the most effective way to ensure that that didn't happen was to talk to [Putin] directly and tell him to cut it out, and there were going to be some serious consequences if he didn't."[68]

Harsh U.S. responses only intensified with Biden, who demanded only a single topic on the agenda of his first summit with Putin in June 2021: "Biden's single in-person opportunity to get through

---

[65]White House, "Remarks by President Obama and President Xi Jinping after Bilateral Meeting."
[66]Ellen Nakashima, "Following U.S. Indictments, China Shifts Commercial Hacking away from Military to Civilian Agency," *Washington Post*, November 30, 2015, https://www.washingtonpost.com/world/national-security/following-us-indictments-chinese-military-scaled-back-hacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html
[67]Email chain with Daniel and Painter.
[68]White House, "Press Conference by the President," December 16, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/16/press-conference-president

to Putin personally was mainly about the threat of ransomware, rather than the more apocalyptic issues of nuclear arms control or Putin's clear belief that Ukraine was not a legitimate country."[69] Biden followed up with Putin to ensure his message was clear, telling reporters that, "when a ransomware operation is coming from his soil, even though it's not sponsored by the state, we expect him to act."[70] Later, Biden also personally warned Xi that China must not interfere in the 2024 U.S. election.[71]

National Cyber Strategies. Trump's 2018 strategy pivoted away from the generic concerns of the baseline period to complain that "Russia, China, Iran, and North Korea all use cyberspace as a means to challenge the United States … often with a *recklessness* they would never consider in other domains."[72] The Biden 2023 strategy concurred that China, Russia, Iran, and North Korea "are aggressively using advanced cyber capabilities to pursue objectives that run counter to our interests and broadly accepted international norms. Their reckless disregard for the rule of law and human rights in cyberspace is threatening U.S. national security and economic prosperity."[73]

Norms were still mentioned, but more as established reality which needs enforcing rather than an ongoing challenge. The 2026 Trump strategy is rooted in grievances against rivals, promising America will "act swiftly, deliberately, and proactively to disable cyber threats to America."[74]

---

[69]David E. Sanger, *New Cold Wars: China's Rise, Russia's Invasion, and America's Struggle to Defend the West* (New York: Crown, 2024), p. 164.
[70]Grace Segers, "Biden Speaks to Putin after Latest Ransomware Attacks," *CBS News*, July 9, 2021, https://www.cbsnews.com/news/biden-putin-ransomware-attacks/
[71]Sean Lyngaas and MJ Lee, "Exclusive: Xi Promised Biden China Wouldn't Interfere in 2024 Election," *CNN*, January 31, 2024, https://edition.cnn.com/2024/01/30/politics/xi-biden-china-us-2024-election/index.html
[72]White House, "National Cyber Strategy," September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, emphasis added.
[73]White House, "National Cybersecurity Strategy," March 2023, https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[74]White House, "President Trump's Cyber Strategy for America," March 2026, https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf

National Security Strategies. The top-level national security strategies follow a similar pattern, with later strategies citing actualities, not possibilities, and promising aggressive responses. The change is especially marked in the two Obama national security strategies, five years apart and issued by the same president. In the baseline period, the first (2010) warned generically about "asymmetric threats, such as those that target our reliance on space and cyberspace."[75] The 2015 strategy required protecting "against cyber-theft of trade secrets for commercial gain whether by private actors or the Chinese government"[76]

The Trump 2017 strategy had the same message, while the Biden 2022 strategy is clear that because cyberattacks "have been used by countries, such as Russia, to undermine countries' ability to deliver services to citizens and coerce populations … we will respond decisively with all appropriate tools of national power to hostile acts in cyberspace."[77]

Mentions in State of the Union Addresses. The president's annual State of the Union (SOTU) shows more variance without indication of new strategic interactions. Clinton first mentioned cybersecurity, in passing, in his 2000 SOTU.[78] It was mentioned on and off again over the years but only meaningfully in Biden's 2021 speech: "I responded directly and proportionally to Russia's interference in our elections and the cyberattacks on our government and our business."[79]

Mentions in Other Presidential Speeches. Other presidential speeches were more consistent.

---

[75]White House, "National Security Strategy," May 2010, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf, p. 17.
[76]White House, "National Security Strategy," February 2015, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf
[77]White House, "National Security Strategy," October 2022, https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.
[78]William J. Clinton, "State of the Union Address," January 27, 1998, https://teachingamericanhistory.org/document/state-of-the-union-address-1998/
[79]White House, "Remarks by President Biden in Address to a Joint Session of Congress," April 28, 2021, https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2021/04/29/remarks-by-president-biden-in-address-to-a-joint-session-of-congress/

At a major speech in 2015, Obama called out North Korea's disruption of Sony Pictures Entertainment as well as "hackers from China and Russia" going after the defense industrial base.[80] It was one of the last presidential speeches to fret about a lack of norms and a digital "Wild West." Biden used a 2021 speech, after the Colonial Pipeline ransomware event (which disrupted the major petroleum pipeline to the U.S. northeast) to note "we have been in direct communication with Moscow about the imperative for responsible countries to take decisive action against these ransomware networks," and promised the U.S. would "disrupt their ability to operate."[81] Soon after, Biden warned that "if we end up in a war, a real shooting war with a major power, it's going to be as a consequence of a cyber breach of great consequence."[82]

Mentions in Speeches by Secretaries of Defense. Speeches by defense secretaries, which had called out specific incidents in the initial period, became surprisingly blander.

In October 2012, defense secretary Leon Panetta called out past cyber incidents, such as the Shamoon attack which disrupted Saudi Aramco and Qatari RasGas and Operation Ababil targeting of U.S. financial institutions, but did not officially blame the perpetrator, Iran.[83] Other cyber-related speeches by defense secretaries generally expressed only broad concerns about adversaries or focused on internal Pentagon priorities.

---

[80]White House, "Remarks by the President at the Cybersecurity and Consumer Protection Summit," February 13, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

[81]White House, "Remarks by President Biden on the Colonial Pipeline Incident," May 13, 2021, https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/

[82]White House, "Remarks by President Biden at the Office of the Director of National Intelligence," July 27, 2021, https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2021/07/27/remarks-by-president-biden-at-the-office-of-the-director-of-national-intelligence/

[83]Thom Shanker and David Sanger, "U.S. Suspects Iran Was Behind a Wave of Cyberattacks," *New York Times*, October 13, 2012, https://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html

Mentions in Speeches by Secretaries of State. Speeches from U.S. secretaries of state showed more variability.

In 2015, John Kerry issued one of the final refrains on the need for cyber norms and the role of international law.[84] Norm turbulence ends after that, as policymakers came to understand the new period of strategic interaction. Mike Pompeo in 2020 not only called out Chinese cyber operations, and in a far cry from the oblique references of Secretary Clinton in the Aurora case a decade earlier, specifically attributing to the Chinese Ministry of State Security.[85]

Other Major Statements, Articles, and Op-Eds. Tom Bossert, then Trump's homeland security advisor, wrote an op-ed to publicly attribute North Korea as the source of the 2017 WannaCry attack, which severely disrupted computers around the world: "North Korea has acted especially badly, largely unchecked, for more than a decade, and its malicious behavior is growing more *egregious*. WannaCry was *indiscriminately reckless*."[86]

In 2021, after the ransomware disruption of Colonial Pipeline, deputy national security advisor Anne Neuberger wrote an unprecedented letter to corporate executives and business leaders, urging them to take steps to protect themselves from ransomware.[87] The following year, Chris

[84]John Kerry, Secretary of State, "An Open and Secure Internet: We Must Have Both," Department of State, May 18, 2015, https://2009-2017.state.gov/secretary/remarks/2015/05/242553.htm
[85]Michael R. Pompeo, Secretary of State, "Silicon Valley and National Security" (speech, Department of State, January 13, 2020), https://2017-2021.state.gov/technology-and-the-china-security-challenge/index.html
[86]Thomas P. Bossert, "It's Official: North Korea Is Behind WannaCry," *Wall Street Journal*, December 18, 2017 https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537, emphasis added.
[87]Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, memo to corporate executives and business leaders, "What We Urge You to Do to Protect against the Threat of Ransomware," White House, June 2, 2021, https://bidenwhitehouse.archives.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf

Inglis, the White House national cyber director, co-authored an article on the need to have "shields up" against Russian attacks linked to the recent full-scale invasion of Ukraine.[88]

Apex policymakers also made major statements about critical vulnerabilities that needed to be patched, which are nearly entirely overlooked in international relations. For example, Michael Daniel, Obama's cyber coordinator, wrote about the Heartbleed vulnerability in 2014,[89] while Neuberger repeatedly stressed the importance of patching critical Microsoft Exchange[90] and log4j vulnerabilities in 2021.[91]

Major Pronouncements About Escalation and Restraint. In the new period of strategic interaction, policymakers indicated the end of their prior restraint.

Even though Sony Pictures Entertainment was not part of critical infrastructure, after it was disrupted in 2014, Obama responded personally, warning "we cannot have a society in which some dictator someplace can start imposing censorship here in the United States." Unprecedentedly, the president himself confirmed the attribution to North Korea.[92] Obama's tone further sharpened after Russian interference in the 2016 elections, again even though elections were also not part of U.S.

[88]Jen Easterly and Chris Inglis, "'Shields Up': The New Normal in Cyberspace," *CyberScoop*, June 6, 2022, https://cyberscoop.com/shields-up-easterly-inglis-op-ed/
[89]Michael Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities," White House, April 28, 2014, https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities/.
[90]White House, "Statement by Deputy National Security Advisor for Cyber and Emerging Technologies Anne Neuberger on New Microsoft Exchange Patches," April 13, 2021, https://www.presidency.ucsb.edu/documents/statement-deputy-national-security-advisor-for-cyber-emerging-technologies-anne-neuberger.
[91]Jack Gillum and Jennifer Jacobs, "Some Federal Systems Affected by Software Flaw, Official Says," *Bloomberg Law*, December 16, 2021, https://news.bloomberglaw.com/privacy-and-data-security/some-federal-systems-affected-by-software-flaw-official-says.
[92]White House, "Remarks by the President in Year-End Press Conference," December 19, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference

critical infrastructure. Obama later brandished to Putin that "frankly we've got more capacity than anybody, both offensively and defensively."[93]

The first Trump administration unsurprisingly leaned into this muscular theme, with national security advisor John Bolton warning that because "our hands are not tied as they were in the Obama administration," the United States would "demonstrate to adversaries that the cost of their engaging in operations against us is higher than they want to bear."[94] A statement from the Biden White House in 2021 laid out further actions to "impose costs" for China's "irresponsible and destabilizing behavior in cyberspace," especially a global incident from a Chinese cyber-intelligence team, nicknamed Hafnium.[95]

Statements from Bilateral Processes. Cyber went from being hardly mentioned in the readouts of earlier U.S.-China Strategic and Economic Dialogues to being, in 2013, featured several times before any other security issues were mentioned even once.[96] Cyber was cited 17 times by senior officials in a background briefing in 2014[97] and another 15 times in 2015 (compared to only six mentions for climate, another Obama priority).[98] In the 2016 joint bilateral outcome document,

[93]White House, "Press Conference by President Obama after G20 Summit," September 5, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/09/05/press-conference-president-obama-after-g20-summit

[94]John Bolton, National Security Advisor, "Transcript: White House Press Briefing on the National Cyber Strategy," Grabien News, September 20, 2018 https://news.grabien.com/makingnews/transcript-white-house-press-briefing-national-cyber-strateg

[95]White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," July 19, 2021, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

[96]Department of State, "U.S.-China Strategic and Economic Dialogue: Outcomes of the Strategic Track," July 12, 2013, https://2009-2017.state.gov/r/pa/prs/ps/2013/07/211861.htm

[97]Department of State, "Background Briefing on the Strategic and Economic Dialogue," July 7, 2014, https://2009-2017.state.gov/r/pa/prs/ps/2014/07/228852.htm

[98]Department of State, "Background Briefing on the U.S.-China Strategic and Economic Dialogue," June 22, 2015, https://2009-2017.state.gov/r/pa/prs/ps/2015/06/244085.htm

cybersecurity is the first topic mentioned, before nonproliferation, anti-corruption, and nuclear security.[99]

Issuance of New Policies. At least six (of the roughly 25) White House cyber-related executive orders and policy directives were issued directly a result of adversary operations.

- EO 13691 (2015) created new organizations for information sharing and attribution as "a direct response" to North Korea's disruption of Sony.[100]
- EO 13694 (2015) declared that malicious cyber activities created a national emergency, to authorize sanctions and other measures.[101]
- NSPM 13 (2018) expanded authorities to conduct cyber operations, which the national security advisor later tied to adversary behaviors like WannaCry and NotPetya (two global cyber disruptions, by North Korean and Russia, respectively) and Chinese theft of intellectual property.[102]
- EO 14028 (2021) instituted major changes to federal cybersecurity and was a "100 percent correlation with SolarWinds," the major Russian espionage campaign.[103]
- NSM-5 (2021) improved security of industrial control systems, driven by the ransomware disruption of the JBS meat processing company.[104]

[99]Department of State, "U.S.-China Strategic and Economic Dialogue: Outcomes of the Strategic Track," June 7, 2016, https://2009-2017.state.gov/r/pa/prs/ps/2016/06/258146.htm
[100]Author discussion with Rob Knake, former deputy national cyber director, February 11, 2026.
[101]"Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," *Federal Register*, April 1, 2015, https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities
[102]Shannon Vavra, "U.S. Ramping Up Offensive Cyber Measures to Stop Economic Attacks, Bolton Says," *CyberScoop*, June 11, 2019, https://cyberscoop.com/john-bolton-offensive-cybersecurity-not-limited-election-security/
[103]Author discussion with Knake.
[104]Author discussion with Brian Scott, former deputy assistant national cyber director, March 20, 2026.

- EO 14390 (2026) detailed actions to counter cybercrime and fraud, noting that "foreign regimes provide willing or tacit state support to cybercrime and predatory schemes."[105]

Use of Hotlines and Other Crisis Communication Channels.

In late October 2016, Obama used a dedicated hotline, set up several years earlier, to warn the Kremlin that the United States considered the election interference as a grave national security matter. Rather than handwringing over rules of the road, he warned the Kremlin that "international law, including the law for armed conflict, applies to actions in cyberspace … We will hold Russia to those standards."[106]

Part 4.2: Escalation as Reflected in Deeds. With their deeds policymakers have shown they have interpreted adversary behavior as crossing thresholds, establishing a new strategic interaction. While the first half are defensive, the last half are intensifiers, institutionalizing offensive capacity and encouraging its use.

Creation and Invocation of National-Level Response Processes. Incidents needing White House attention went from zero in the baseline period to being so frequent by 2016 that the White House formalized a standing Cyber Response Group in the NSC. That was driven in part by North Korea's disruption of Sony two years before,[107] which led to "months of fevered efforts to

[105]White House, "Combating Cybercrime, Fraud, and Predatory Schemes against American Citizens," March 6, 2026, https://www.whitehouse.gov/presidential-actions/2026/03/combating-cybercrime-fraud-and-predatory-schemes-against-american-citizens/
[106]William M. Arkin, Ken Dilanian, and Cynthia McFadden, "What Obama Said to Putin on the Red Phone about the Election Hack," *NBC News*, December 19, 2016, https://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116
[107]White House, "Presidential Policy Directive—United States Cyber Incident Coordination," July 26, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

implement lessons across government, including the creation of the Cyber Threat Intelligence Integration Center to ensure that the White House could get quick assessments of future attacks."[108]

By 2021, the new Biden administration created a special position, a deputy national security advisor for cyber, filled by Anne Neuberger. From the very first day of the administration she led major incident response such as the Russian intelligence services' large-scale and highly sophisticated espionage intrusion into SolarWinds[109] and the Colonial Pipelines ransomware, updating citizens from behind White House podium.[110] During the Change Healthcare ransomware incident of 2024, Neuberger led the NSC Deputies Committee for over a week to handle the crisis.[111]

White House Cyber Staffing. From about 20 staffers in the period of initial strategic interaction, by the time of the Biden administration, the number surged to roughly 80 (about 17 in the NSC plus over 60 in the Office of the National Cyber Director (ONCD)), excluding those working on cybersecurity for Federal systems.[112] According to one deputy national cyber director, the Biden administration may not have expanded so extravagantly if not for the SolarWinds incident.[113]

[108]John P. Carlin and Garrett M. Graff, *Dawn of the Code War: America's Battle against Russia, China, and the Rising Global Cyber Threat* (New York: PublicAffairs, 2018), p. 343.
[109]Julian E. Barnes and David E. Sanger, "White House Announces Senior Official Is Leading Inquiry into SolarWinds Hacking," *New York Times*, February 10, 2021, https://www.nytimes.com/2021/02/10/us/politics/biden-russia-solarwinds-hacking.html
[110]White House, "Press Briefing by Press Secretary Jen Psaki, Homeland Security Advisor and Deputy National Security Advisor Dr. Elizabeth Sherwood-Randall, and Deputy National Security Advisor for Cyber and Emerging Technologies Anne Neuberger," May 10, 2021, https://bidenwhitehouse.archives.gov/briefing-room/press-briefings/2021/05/10/press-briefing-by-press-secretary-jen-psaki-homeland-security-advisor-and-deputy-national-security-advisor-dr-elizabeth-sherwood-randall-and-deputy-national-security-advisor-for-cyber-and-emerging/
[111]John Sakellariadis, "Hospitals Are Pleading for Help. The NSC May Be Close to Giving It," *Politico*, March 4, 2024, https://www.politico.com/newsletters/weekly-cybersecurity/2024/03/04/hospitals-are-pleading-for-help-the-nsc-may-be-close-to-giving-it-00144647
[112]Author discussion with Knake.
[113]Author discussion with Knake.

Declaring Emergencies. No longer were cyber incidents merely serious, but not official emergencies. Obama issued EO 13694 in 2015 to declare a national emergency to unlock special authorities such as sanctions while the governors of Colorado[114] and Louisiana[115] declared emergencies to deal with local ransomware incidents. After the ransomware of Colonial Pipeline, 17 states declared emergencies.[116]

Convening of Major Summits. Fifteen years since the first White House cyber summit, Obama personally convened another in 2015 at Stanford University.[117] The Biden administration convened five more for the Counter Ransomware Initiative, involving over 60 nations[118] plus a sixth on workforce issues.[119]

Applying Sanctions. In the baseline period, America had no program to issue cyber-related sanctions, which did not start until 2012. By 2015 and 2016, there were just under 20 cyber-related sanctions delegations per year. In the first Trump administration, the average bumped to over 50 and 35 under Biden.[120]

Issuing Indictments. Indictments have a more variable curve than sanctions, but like sanctions, that they are happening at all is an important difference from the baseline. The Obama

[114]Benjamin Freed, "What Colorado Learned from Treating a Cyberattack Like a Disaster," *StateScoop*, May 15, 2019, https://statescoop.com/what-colorado-learned-from-treating-a-cyberattack-like-a-disaster/
[115]State of Louisiana, "State of Emergency—Cybersecurity Incident," July 24, 2019, https://gov.louisiana.gov/assets/EmergencyProclamations/115-JBE-2019-State-of-Emergency-Cybersecurity-Incident.pdf
[116]James Walker, "Cyber Attack on Colonial Pipeline Leads to Emergency Declaration in 17 States," *Newsweek*, May 10, 2021, https://www.newsweek.com/cyber-attack-colonial-pipeline-emergency-declaration-1589936
[117]White House, "Remarks by the President at the Cybersecurity and Consumer Protection Summit."
[118]White House, "FACT SHEET: Biden-Harris Administration Convenes Fourth Global Gathering to Counter Ransomware," October 2, 2024, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/10/02/fact-sheet-biden-%E2%81%A0harris-administration-convenes-fourth-global-gathering-to-counter-ransomware/
[119]University of California, Santa Barbara, *The American Presidency Project*, https://www.presidency.ucsb.edu/advanced-search.
[120]Jason Bartlett and Megan Ophel, "Sanctions by the Numbers: Spotlight on Cyber Sanctions," Center for a New American Security (CNAS), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber

administration issued 10 indictments in 2016, with the average later climbing to nearly 30 a year between 2017 and 2019. It later dropped to an average of four per year in 2020 to 2023, [121] then leapt again to 25 in 2024 and 18 in 2025.[122]

Spending on Military Cyber Operations: The deeds from here and below are "intensifiers," as they all expand bureaucratic capacity for offensive and countering operations and encourage their use, and accordingly more likely to ratchet cyber conflict at higher objective intensities.

Publicly announced cyber-related spending within the DoD has grown nearly every year, as shown in Figure 6, both overall and as growth year-over-year, in constant dollars.

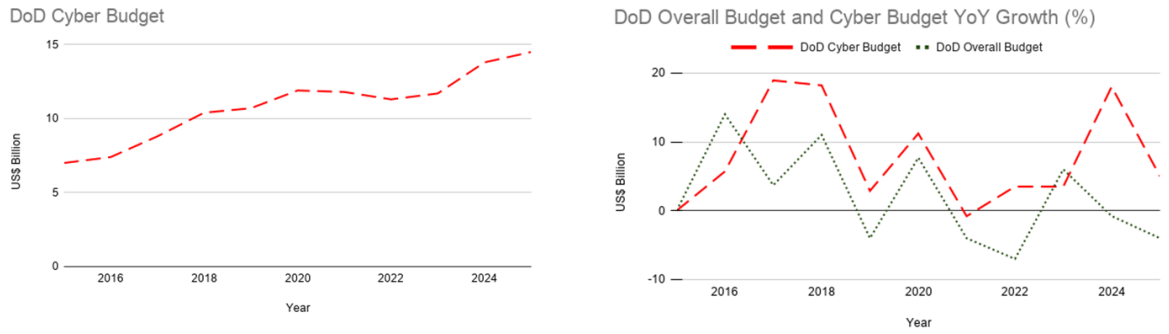


Figure 6: DoD Cyber Budget both overall (left, in constant dollars) and year-over-year growth (right)

Creation of Military Cyber Commands. For two decades, every major cyber organization created by the U.S. military was in response to a recent cyber incident, only one of which was

[121]Trevor Logan and Pavak Patel, "Data Visualization: U.S. Sanctions against Malicious Cyber Actors," Foundation for Defense of Democracies, April 20, 2020, https://www.fdd.org/analysis/visuals/2020/02/28/data-visualization%3A-us-sanctions-against-malicious-cyber-actors/, and Primary data collected by the authors from indictments identified as state-sponsored cybercrime among the results of a "cybercrime" keyword search, "Press Releases," Department of Justice, (accessed February 26, 2026), https://www.justice.gov/news/press-releases?keys=cybercrime

[122] Trevor Logan and Pavak Patel, "Data Visualization: U.S. Sanctions against Malicious Cyber Actors," Foundation for Defense of Democracies, April 20, 2020, https://www.fdd.org/analysis/visuals/2020/02/28/data-visualization%3A-us-sanctions-against-malicious-cyber-actors/ ; and primary data collected by the authors from indictments identified as state-sponsored cybercrime among the results of a "cybercrime" keyword search, "Press Releases," Department of Justice, (accessed February 26, 2026), https://www.justice.gov/news/press-releases?keys=cybercrime

disruptive and two of which were ultimately from non-states. While these are not evidence of a shift in strategic interaction post-2012, they are included here both as examples of intensifiers, institutionalizing bureaucratic capacity and because they feature in the case studies.

After the Morris Worm of 1988 (written by a graduate student), the DoD funded the creation of the first Computer Emergency Response Team.[123] The formation of the Joint Task Force - Computer Network Defense (JTF-CND) in 1998 was a direct response to the Solar Sunrise incident.[124] U.S. Cyber Command was created a decade later in large part due to the lessons of Buckshot Yankee, the Russian intrusion into classified DoD networks in 2008.[125]

Military Cyber Manpower. The creation of the new commands discussed above was not just a reorganization of the existing workforce but represented substantial additional investment with two orders of magnitude more personnel during the period of new strategic interaction, as shown in Table 3.

Table 3: Cyber Personnel in Major US Cyber Commands

Year	Organization	# of Personnel
1998	JTF-CND	Started with ~24[126]
2000	JTF-CNO	~150[127]
2012	U.S. Cyber Command	931[128]
2018	U.S. Cyber Command	6200[129]

[123]Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2013* (Arlington, VA: Cyber Conflict Studies Association, 2013), p. 68.
[124]Healey, *A Fierce Domain*, p. 44.
[125]Brian Knowlton, "Military Computer Attack Confirmed," *New York Times*, August 25, 2010, https://www.nytimes.com/2010/08/26/technology/26cyber.html
[126]Healey, *A Fierce Domain*, p. 60.
[127]Healey, *A Fierce Domain*, p. 60.
[128]Keith B. Alexander, "Building a New Command in Cyberspace," *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 3–12, https://www.jstor.org/stable/26270554.
[129]Mark Pomerleau, "Here's How DoD Organizes Its Cyber Warriors," *Fifth Domain*, September 13, 2018, https://www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/

2022	U.S. Cyber Command	~6800[130]

More Permissive Military Operating Concepts. Locking in the new strategic interaction, the United States promulgated a new military operational concept to remove constraints and demand active contention with adversaries. Just five years after Pentagon officials bragged about U.S. restraint, John Bolton, the national security advisor, warned the U.S. embraced an "aggressive offense" as its "hands were not tied" as they had been earlier.[131]

More Permissive Congressional Authorities. Congress, citing Russia's interference into U.S. elections, confirmed the new strategic interaction, further reduced constraints by authorizing the president to "take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter" any "active, systematic, and ongoing" campaigns by Russia, China, North Korea or Iran.[132]

More Permissive Law-Enforcement Operating Concepts. The Pentagon shift towards more active contention with adversaries was matched by changes at the Department of Justice. Lisa Monaco, the deputy attorney general, later described the new strategy that extradition and prosecution "is not the be all and end all" for prosecutors, who "every single time [should] ask yourselves can I take a disruptive action?"[133]

[130]Estimated based on growth of about 10 percent, from 133 to 147 operational teams; see Posture Statement of Gen. Paul M. Nakasone, Commander, U.S. Cyber Command, before the Senate Committee on Armed Services, 117th Cong., 2d sess., April 5, 2022., https://www.armed-services.senate.gov/imo/media/doc/5%20Apr%20SASC%20CYBERCOM%20Posture%20Statement%20(GEN%20Nakasone)%20-%20FINAL.pdf.
[131]Bolton transcript, *Grabien News*.
[132]John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong. (2017–2018), August 13, 2018, https://www.congress.gov/bill/115th-congress/house-bill/5515/text
[133]Lisa Monaco, Deputy Attorney General, remarks at the 2024 Munich Cyber Security Conference, Department of Justice, March 14, 2024, YouTube video, https://www.youtube.com/watch?v=sBk28AOSDr0

More Aggressive Military Operations. The never-subtle Bolton announced that the United States "will impose costs on you until you get the point."[134] The United States shifted "more toward offense … with the placement of potentially crippling malware inside the Russian system at a depth and with an aggressiveness that had never been tried before."[135] Because disruptions no longer needed to be approved by the president, U.S. operations, according to one senior intelligence official, became "far, far more aggressive over the past year … at a scale that we never contemplated a few years ago."[136]

General Paul Nakasone, then-commander at U.S. Cyber Command, told Congress that "[e]nabled by changes in law and policy, we have produced defensive and offensive operational successes." The "new operating construct" enabled "defending against malicious cyberspace activities as far forward as possible,"[137] such as disrupting a Russian criminal ransomware group suspected of planning a disruption of the 2020 election.[138] General Nakasone said that compared to earlier,

[134]Warren P. Strobel, "Bolton Says U.S. Is Expanding Offensive Cyber Operations," *Wall Street Journal*, June 11, 2019, https://www.wsj.com/articles/bolton-says-u-s-is-expanding-offensive-cyber-operations-11560266199
[135]David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *New York Times*, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html
[136]Ibid.
[137]Gen. Paul M. Nakasone, commander, U.S. Cyber Command, statement before the House Committee on Armed Services, Subcommittee on Intelligence, Emerging Threats, and Capabilities, March 4, 2020, https://www.congress.gov/116/meeting/house/109083/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20190313.pdf
[138]Ellen Nakashima, "Cyber Command Has Sought to Disrupt the World's Largest Botnet, Hoping to Reduce Its Potential Impact on the Election," *Washington Post*, October 9, 2020, https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html; Julian E. Barnes, "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *New York Times*, February 26, 2019, https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html

when "the government saw ransomware attacks as the responsibility of law enforcement,"[139] there was now a military role, including the disruption of a Russian-linked ransomware group.[140]

Creation of Dedicated Law Enforcement Organizations. The new operating concepts at Justice mentioned above led to the creation of new organizations, the Ransomware and Digital Extortion Task Force.[141]

More Aggressive Law-Enforcement Countering Operations. These new law-enforcement concepts and organizations disrupted adversaries in unthinkable ways during the baseline period. One chief federal prosecutor stressed how such operations exemplified the "forward-leaning, disruption-first approach we are taking to address this threat," and that Justice would "pull no punches."[142] Earlier, there had only been a handful of disruptive operations, such as botnet takedowns in 2010, 2011, 2014 and 2017. With the new focus on disruption, there were at least eight over the next four years.[143]

Part 5: Case Studies

[139]Julian E. Barnes, "U.S. Military Has Acted against Ransomware Groups, General Acknowledges," *New York Times*, December 5, 2021, https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html

[140]Ellen Nakashima and Dalton Bennett, "A Ransomware Gang Shut Down after Cybercom Hijacked Its Site and It Discovered It Had Been Hacked," *Washington Post*, November 3, 2021, https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html

[141]Department of Justice, "Advancing the Department's Response to Cyber Threats, 2021–2025," https://www.justice.gov/archives/media/1385296/dl?inline

[142]Department of Justice, "Justice Department Announces Coordinated Disruption Actions against BlackSuit (Royal) Ransomware Operations," August 11, 2025, https://www.justice.gov/opa/pr/justice-department-announces-coordinated-disruption-actions-against-blacksuit-royal

[143]Department of Justice, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists DarkSide," June 7, 2021, https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

Case studies of North Korea, Russia, and China further highlight how cyber conflict has worsened from the baseline strategic interactions, giving more fine-grained detail of new strategic interactions than the words-and-deeds analysis.

Part 5.1: Case Study of U.S. Policymaker Perception of North Korean-linked Attacks

There was a clear shift in the words and deeds of apex policymakers in dealing with North Korea, matching Figure 4.3.

Phase 1, Baseline (1990s to ~2014). In the period of initial strategic interaction, North Korea conducted attacks against South Korea and the United States, even disrupting the White House and Treasury Department websites. However, the only response from the U.S. government was blandly technical ("all federal Web sites were back up and running") without calling out North Korea or labeling the attacks as unacceptable.[144]

Phase 2, Escalation (2014-). This nonchalance shifted after perceived vertical escalation by North Korea. The NSC Deputies Committee struggled to develop responses to the 2014 North Korean hack of Sony ("we were shocked at how few tools the United States truly possessed under these circumstances")[145] with Obama himself confirming the attribution to North Korea and promising a proportional response.[146] This incident drove new executive orders and formalization of the Cyber Response Group in the White House and the Cyber Threat Intelligence Integration

[144]Choe Sang-Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *New York Times*, July 9, 2009, https://www.nytimes.com/2009/07/10/technology/10cyber.html.
[145]Carlin and Graff, *Dawn of the Code War*, pp. 307–341.
[146]David E. Sanger, Michael S. Schmidt, and Nicole Perlroth, "Obama Vows a Response to Cyberattack on Sony," *New York Times*, December 19, 2014, https://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html; "Obama: Sony Hack Was Cyber-Vandalism, Not an 'Act of War,'" *NBC News*, December 21, 2014, https://www.nbcnews.com/news/world/obama-sony-hack-was-cyber-vandalism-not-act-war-n272541

Center.[147] As Lisa Monaco, Obama's homeland security advisor put it, "Sony made clear we needed to yank all that stuff up and put it into high gear."[148]

Three years to the day after Obama's response to Sony, Tom Bossert, the White House homeland security advisor, formally attributed the 2016 WannaCry attack to North Korea in an op-ed[149] and from the podium in the White House press briefing room, using vivid words, calling it "reckless" six times and North Korean behavior as "growing more egregious."[150] Since then, the U.S. reactions have generally plateaued with indictments but no qualitatively different response to operations like the attempted theft of nearly $1 billion from the Bank of Bangladesh.[151]

Part 5.2: Case Study of U.S. Policymaker Perception of Russia and Russia-Nexus Groups.

An assessment of the U.S. response to cyber campaigns from Russia-nexus threat actors demonstrates two distinct higher-then-higher shifts from the baseline interaction, in line with Figure 4.5. Policymaker's concerns of Russian cyber behavior only came after erosion of the geopolitical situation.

Phase 1, Restraint (1980s to 2007). In this baseline period, Russian activity was generally treated as routine within accepted international practice. There were significant "wakeup calls," such Russian hacktivist support to Serbia during Operation Allied Force in 1999,[152] but none so severe

[147]Office of the Director of National Intelligence (ODNI), https://www.odni.gov/index.php/ctiic/who-we-are/history.
[148]Carlin and Graff, *Dawn of the Code War*, p. 341.
[149]Bossert, "It's Official: North Korea Is Behind WannaCry."
[150]The American Presidency Project, "Press Briefing by Assistant to the President for Homeland Security and Counterterrorism Tom Bossert and Assistant Secretary of Homeland Security for Cybersecurity and Communications Jeanette Manfra on the Attribution of the WannaCry Malware Attack to North Korea," December 19, 2017, https://www.presidency.ucsb.edu/documents/press-briefing-assistant-the-president-for-homeland-security-and-counterterrorism-tom
[151]Department of Justice, "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," press release, September 6, 2018, https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.
[152]Healey, *A Fierce Domain*, pp. 137-141.

the United States felt it needed aggressive responses. These may have caused an initial shift in strategic interactions around 1998, however even the major Moonlight Maze intrusion was considered acceptable geopolitical espionage.

Phase 2, Initial escalation (2007 to 2014). The 2007 cyberattacks against Estonia by Russian-speaking hactivists started a transition to a new strategic interaction, a vertical escalation from espionage to large-scale disruption. It was the first geopolitically important cyber campaign, knocking a NATO country offline. NATO took unprecedented steps after this attack on a member state, addressing cyber threats for the first time in its Bucharest Declaration and creating a cyber center in Tallinn within a year of the attack, a step the alliance had earlier resisted.[153] Russian cyberattacks against Georgia in 2008 were another wakeup call, as the Georgian leadership was essentially unable to communicate internally or communicate about the ongoing invasion.[154]

That same year, the Russian espionage incident named Operation Buckshot Yankee penetrated classified military systems and "marked a turning point in U.S. cyberdefense strategy," according to the deputy secretary of defense.[155] Despite only being espionage, which failed to steal any military secrets, this campaign helped drive the creation of U.S. Cyber Command, as the Pentagon "saw an environment that was much more intensely competitive. Unless we escalated, others would impact DoD's ability to operate."[156] Around the same time, the first reports started to

[153]NATO, "Bucharest Summit Declaration," April 3, 2008, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2008/04/03/bucharest-summit-declaration
[154]US Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," https://github.com/johnbumgarner/published_articles_and_research_papers/blob/master/US-CCU%20Reports/US-CCU%20Georgia%20Cyber%20Campaign%20Overview.pdf
[155]Lynn, "Defending a New Domain."
[156]Author interview with Bob Butler, former deputy assistant secretary of defense for cyber policy, via video call, April 29, 2024.

publicly emerge of Russian and Chinese mapping U.S. infrastructure, including the electrical grid, in preparation for a future attack.[157]

Phase 3, Further escalation (2014-). A second, even more intense shift followed the Russian annexation of Crimea in 2014. Russian cyber disruptions were no longer only aimed at their "near abroad" of former Soviet states but at the United States itself, a classic example of horizontal escalation. Earlier Russian disruption of the Ukrainian electrical grid took on a far darker tone, as more reports emerged of their growing presence in the U.S. grid.[158]

The vertical escalation of Russia's interference in the 2016 presidential election delivered a more direct and severe shock. The unprecedented American response included use of the White House-Kremlin hotline, declaration of persona non grata, and the imposition of sanctions. In a clear sign of the new interaction, national security advisor Susan Rice later wrote poignantly that responding was "a uniquely challenging policy problem … We were operating in substantially uncharted territory where the stakes couldn't be higher."[159]

Yet further traumas were on the way, including the 2017 NotPetya disruption by Russian military intelligence, which the White House called out as a "reckless and indiscriminate cyber-attack that will be met with international consequences."[160] The Biden administration declared the 2021 SolarWinds intrusion as a "significant cyber event," convening a Cyber Unified Coordination

[157]Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, April 8, 2009, https://www.wsj.com/articles/SB123914805204099085
[158]Nicole Perlroth, "Russian Hackers Targeting Oil and Gas Companies," *New York Times*, June 30, 2014, https://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html
[159]Susan Rice, *Tough Love: My Story of the Things Worth Fighting For* (New York: Simon and Schuster, 2019), p. 449.
[160]White House, "Statement from the Press Secretary," February 15, 2018, https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/

Group to respond.[161] Toria Nuland, the State Department undersecretary of policy recalled that it "really woke people up" and "crystallized minds… that we were going to have to be pretty strong right back if we wanted to get Putin's attention."[162] That aggressive response included substantial sanctions, even though the campaign was geopolitical espionage, which the U.S. had long signaled was fair game.[163]

From 2018 onward, ransomware attacks were a persistent challenge from Russia. The 2020 Colonial Pipeline attack, attributed to a Russia-based cybercriminal group, forced governors in 17 states to declare emergencies. A similar attack later targeted Change Healthcare, a single point of failure for medical claims, so disrupted "critical operations and payment flows across the healthcare sector"[164] that the NSC Deputies Committee convened every day for over a week.[165] After another disruption, at JBS, the world's largest meat processor, Biden's press secretary said the White House was "engaging directly with the Russian government on this matter and delivering the message that responsible states do not harbor ransomware criminals."[166]

[161]Cybersecurity and Infrastructure Security Agency (CISA), "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)," January 5, 2021, https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure-security-agency-0

[162]Sanger, *New Cold Wars*, pp. 121, 124.

[163]David E. Sanger and Andrew E. Kramer, "U.S. Imposes Stiff Sanctions on Russia, Blaming It for Major Hacking Operation," *New York Times*, April 15, 2021, https://www.nytimes.com/2021/04/15/world/europe/us-russia-sanctions.html

[164]Arthur Fliegelman and Daniel Stemp, "The Cyberattack on Change Healthcare: Lessons for Financial Stability," Office of Financial Research, November 13, 2024, https://www.financialresearch.gov/briefs/files/OFRBrief-24-05-change-healthcare-cyberattack.pdf

[165]Sakellariadis, "Hospitals Are Pleading for Help."

[166]Bryan Harris, James Politi, Jamie Smyth, and Henry Foy, "Russian Criminal Gang Probably Hacked Meat Supplier JBS, Says White House," *Financial Times*, June 1, 2021, https://www.ft.com/content/00eca8fc-4278-4c98-ace3-5967fe3bbd11?syn-25a6b1a6=1

Biden put personal pressure on Putin over such escalation, dedicating their only summit to the topic of ransomware,[167] with his team later messaging that "Biden underscored the need for Russia to take action to disrupt ransomware groups operating in Russia and … reiterated that the United States will take any necessary action to defend its people and its critical infrastructure."[168]

After disruptions against U.S. grain cooperatives in 2021,[169] the national security advisor convened a small group to develop a quick-look assessment to assess if they violated Biden's demand that Russia stop attacks against U.S. critical infrastructure.[170] Some ransomware incidents, like that against the U.S. subsidiary of ICBC, the major Chinese bank, received little public attention, but drove substantial government responses to address potential systemic risks.[171]

Part 5.3: Case Study on China and Chinese-Nexus Threat Actors

An assessment of the U.S. response to cyber campaigns from China-nexus threat actors also shows two distinct higher-then-higher shifts from the baseline interaction, in line with Figure 4.5, However in contrast to the Russia case study, American cyber concerns *preceded the larger geopolitical shifts*, helping initiate the lasting deterioration of the U.S.-China relationship.

Phase 1, Restraint (Early 2000s to 2012). The United States complained repeatedly about Chinese cyber behavior, but not at the expense of other priorities.[172] There was no major U.S. response to the surge of Chinese patriotic hacking of US government websites tied to the 2001

[167]Michael D. Shear, "Biden Urges Putin to 'Take Action to Disrupt' Russia-Based Hackers behind Ransomware Attacks," *New York Times*, July 9, 2021, https://www.nytimes.com/2021/07/09/us/politics/putin-biden-ransomware-hackers.html
[168]White House, "Readout of President Joseph R. Biden Jr.'s Call with President Vladimir Putin of Russia," July 9, 2021, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/07/09/readout-of-president-joseph-r-biden-jr-call-with-president-vladimir-putin-of-russia-2/
[169]FBI, "Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons," April 20, 2022, https://www.ic3.gov/CSA/2022/220420-2.pdf.
[170]Author discussion with Scott.
[171]Author discussion with a former senior Treasury official involved in cyber response with apex policymakers, July 17, 2026.
[172]Author discussion with Tom Christensen, former deputy assistant secretary of state for East Asia, April 7, 2026.

"Hainan Island incident,"[173] nor to major cyber espionage intrusions such as Titan Rain[174] or the 2007 theft of the blueprints for the Joint Strike Fighter.[175]

Secretary of State Hillary Clinton called out the 2010 Operation Aurora cyber espionage campaign, affecting Google and over 30 other companies, and demanded a Chinese investigation.[176] But, she was apparently on her own: "President Obama, who has repeatedly warned of the country's vulnerability to devastating cyberattacks, has said nothing in public about one of the biggest examples since he took office."[177] Nor did cyber issues feature in the readouts of the top-level talks between the United States and China, the Strategic and Economic Dialogue. The related intrusions into RSA Security and Lockheed Martin, to steal the blueprints of the Joint Strike Fighter, were some of the last which were met with such relative calm.[178]

Phase 2, Breaking Point (2013 to ~2021). By 2012, the U.S. patience was over. In contrast with Russia, there was not a geopolitical spark (like annexing Crimea) or a single incident (election interference) which drove the change, but the collective set of Chinese behavior.

The Obama administration raised Chinese behavior in every meeting with counterparts and initiated more decisive actions, such as the 2014 indictment of five active-duty People's Liberation Army (PLA) military officers for theft of intellectual property,[179] which national security advisor

[173]Eugenio Benincasa, *Before Vegas: The "Red Hackers" Who Shaped China's Cyber Ecosystem* (Zurich: Center for Security Studies, ETH Zurich, 2025).
[174]Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time*, August 25, 2005, https://time.com/archive/6918871/inside-the-chinese-hack-attack/
[175]Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009, https://www.wsj.com/articles/SB124027491029837401
[176]Hillary Rodham Clinton, "Remarks on Internet Freedom."
[177]David E. Sanger and John Markoff, "After Google's Stand on China, U.S. Treads Lightly," *New York Times*, January 14, 2010, https://www.nytimes.com/2010/01/15/world/asia/15diplo.html
[178]William J. Lynn, "Remarks on Department of Defense Cyber Strategy" (address, National Defense University, July 14, 2011), https://www.securityweek.com/william-j-lynn-remarks-department-defense-cyber-strategy-transcript/.
[179]Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014,

Susan Rice considered an "extraordinarily provocative" escalation.[180] She later wrote that "diplomacy had not yielded results. Repeated warnings had failed. I came to Beijing with a strong and clear message: 'If China doesn't stop stealing our stuff, we will sanction you' ... I repeated our position privately at every opportunity, including more diplomatically with President Xi."[181]

The 2015 theft of personnel records by Chinese intelligence from the U.S. Office of Personnel Management (OPM) was especially vivid, sparking anger and personal insult: "There was this sense of feeling violated that really pissed people off," one official told journalist David Sanger, which "dramatically decreased the Obama administration's willingness to assume that Beijing was acting in good faith."[182]

The OPM incident was again exactly the kind of geopolitical intelligence that the United States had said were perfectly legitimate. Yet the White House responded to it as vertical escalation. When announcing a new "aggressive" cyber posture, national security advisor Bolton defended the move in terms of the OPM incident, "the kind of threat to privacy from hostile foreign actors that we're determined to deter," with "powerful deterrence structures that persuade the adversary not to strike in the first place."[183]

The tensions spiraled outside of direct cyber competition. In large part because of cybersecurity concerns, "the Trump administration launched a campaign against Huawei, one of China's largest telecom giants."[184] China saw this as a "major escalation and served as Beijing's own wake-up

https://www.justice.gov/archives/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[180]Carlin and Graff, *Dawn of the Code War*, pp. 267–8.
[181]Rice, *Tough Love*, p. 437.
[182]Sanger, *New Cold Wars*, p. 70.
[183]Bolton transcript, *Grabien News*.
[184]Gloria Xiong and Jessica Chen Weiss, "How China Found Its Most Potent Weapon," *Foreign Affairs*, September/October 2026, https://www.foreignaffairs.com/china/how-china-found-most-potent-weapon-xiong-weiss.

call," responding with "tariffs against carefully selected exports, such as soybeans and energy, from Republican-supporting districts."

Phase 3, Rising Plateau (2021-). Since then, concerns have only continued to grow. Obama's national security advisor Jake Sullivan declared that Chinese operations were "dramatic in their scope and scale and we take them deadly seriously."[185]

The U.S. response to China's 2021 Hafnium attack is indicative, with a range of extraordinary responses, unthinkable in earlier periods. The United States took once-rare-now-routine actions of declaring a significant cyber incident and convening a Cyber Unified Coordination Group. Justice got an unprecedented court order authorizing law enforcement to intrude into victim computers to remove the Chinese malware.[186] Deputy national security advisor Neuberger made an official statement while a broad coalition of allies simultaneously condemned Beijing's actions.[187] Secretary of State Antony Blinken asserted that China's involvement in the hack represented a "pattern of irresponsible, disruptive and destabilizing behavior."[188]

American concerns shifted from espionage to a Chinese group, Volt Typhoon, pre-positioning "to disrupt critical infrastructure operations in the event of geopolitical tensions and/or military conflicts," as national security advisor Sullivan warned governors, yet another unprecedented step.[189] Sullivan later confirmed the White House "sent a clear message to China's leaders that if

---

[185]Jenny Leonard and Courtney McBride, "Sullivan Urges Trump Team to Focus on China Cyberthreats," *Japan Times*, January 14, 2025, https://www.japantimes.co.jp/news/2025/01/14/world/politics/sullivan-trump-china-cyber/

[186]Department of Justice, "Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities," April 13, 2021, https://www.justice.gov/archives/opa/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft-exchange

[187]White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China."

[188]David Smith and Vincent Ni, "US Condemns China for 'Malicious' Cyberattacks, Including Microsoft Hack," *Guardian*, July 20, 2021, https://www.theguardian.com/technology/2021/jul/19/microsoft-exchange-hack-us-biden-administration-china

[189]White House, "Letter to Governors," March 18, 2024, https://www.epa.gov/system/files/documents/2024-03/epa-apnsa-letter-to-governors_03182024.pdf

... they actually took a physically destructive cyberattack in the United States … that there would be severe consequences."[190]

Biden also personally warned Xi Jinping to not interfere in the 2024 election[191] and both the Biden and second Trump administrations have been exceedingly concerned about a widespread Chinese espionage campaign, Salt Typhoon, affecting major telecommunication companies.[192] The Biden response was led by deputy national security advisor Neuberger and driven by a Cyber Unified Coordination Group.[193]

Part 6. Analysis, Implications, and Next Steps

This section includes the analysis of subjective escalation theory and comparison with the other two approaches, alternative explanations and lessons and future research.

Part 6.1. Summary Analysis

Across almost every line of evidence, apex U.S. policymakers, as represented by their words and deeds, recognized a qualitative intensification of strategic interaction after 2012, consistent with Figure 4.3. None of the evidence shows any de-escalation, such as decreased budgets or substantial re-imposition of operational constraints. The North Korea case study also matches Figure 4.3, while the China and Russia case studies each show patterns of a two-step higher-then-higher shift in strategic interaction, consistent with Figure 4.5. In addition, the China case shows how cyber

[190]Jenny Leonard and Courtney McBride, "Sullivan Urges Trump Team to Focus on China Cyber Threats," *Bloomberg*, January 13, 2025, https://www.bloomberg.com/news/articles/2025-01-13/sullivan-urges-trump-team-to-focus-on-china-cyber-threats; Jenny Leonard and Courtney McBride, "Sullivan Urges Trump Team to Focus on China Cyberthreats," *Japan Times*, January 14, 2025, https://www.japantimes.co.jp/news/2025/01/14/world/politics/sullivan-trump-china-cyber/
[191]Lyngaas and Lee, "Exclusive: Xi Promised Biden China Wouldn't Interfere in 2024 Election."
[192]Matt Kapko, "White House Says 9th Telecom Company Hit in Salt Typhoon Spree," *Cybersecurity Dive*, December 27, 2024, https://www.cybersecuritydive.com/news/salt-typhoon-telecom-attacks-lax-security/736233/
[193]Greg Otto, "White House: Chinese Telecom Hacks Have Been in Motion for Years," *CyberScoop*, December 4, 2024, https://cyberscoop.com/salt-typhoon-national-security-council-chinese-spying/

helped drive perhaps the most important geopolitical shift of the century, the U.S. switch from seeing China-as-partner to China-as-competitor. The Russia case flipped the causation, with changes to U.S. perception only coming after the geopolitical rupture of the 2014 annexation of Crimea. None of the case studies show evidence of de-escalation.

Table 4 below summarizes key findings.

Table 4: Assessment of Subjective Escalation Theory

	Finding	**Support**
Formation of Perception of Apex Policymakers	Cyber incidents shape the perceptions of apex policymakers in ways they may perceive as escalation, crossing critical thresholds and leading to new strategic interactions.	Supported across almost all lines of evidence and all case studies.
	Perception of apex policymakers is not formed all at once, but compounds cumulatively over time with spikes after particularly severe incidents.	Supported across almost all lines of evidence and all case studies.
	Perception of apex policymakers is formed by a range of cyber incidents: disruption.	Supported: Mafiaboy attacks; Estonia; Georgia; Shamoon; Ababil; Sony; WannaCry; NotPetya; Colonial Pipelines, Change Healthcare, JBS, ICBC US, and other ransomware attacks.
	Perception of apex policymakers is formed by a range of cyber incidents: preparation for wartime disruption.	Supported: Solar Sunrise (mistakenly), Volt Typhoon.
	Perception of apex policymakers is formed by a range of cyber incidents: espionage.	Supported: Moonlight Maze, Aurora, campaigns of Chinese IP theft, Buckshot Yankee, Aurora, OPM, and SolarWinds.
	Perception of apex policymakers is formed by a range of cyber incidents: incidents from non-states.	Supported: Morris worm; Solar Sunrise; Estonia; Georgia; Mafiaboy attacks; and Colonial Pipelines, Change Healthcare, JBS, ICBC US, and other ransomware attacks.

	Perception of apex policymakers can be driven by vividness of incidents, not only objective factors such as number of victims or economic cost.	Supported: Solar Sunrise, Estonia, Georgia, Buckshot Yankee, OPM, Sony, 2016 election interference.
Responses of Apex Policymakers	Policymakers will respond to the transition to a new period of intensifying strategic interactions with vivid descriptors and call for norms. Once the new strategic interaction is mature, these words will appear far less.	Supported: Such words were common before and after 2012 the transition period around 2012 but have substantially diminished since 2020.
	Responses will not just be within cyberspace but with a range of words and deeds. In a period of intensifying strategic interaction, the range of responses expands over time, possibly very quickly.	Supported across almost all lines of evidence and all case studies.
	Responses are idiosyncratic with only a limited correlation with implicit or explicit thresholds, such as stated red lines.	Supported. Apex policymakers declared espionage for geopolitical purposes to be acceptable then treated OPM and SolarWinds as escalation. Elections and Sony were not considered critical infrastructure when attacked.
	Response can be driven by psychological factors as much as objective.	Supported. Aggressive responses like offensive counteractions against Chinese IP theft are domain of loss: policymakers feel they are falling farther behind so need to double down to regain what was lost. Response to OPM seemed marked by outrage and personal affront. Obama drew a line in response to Sony: *here and no further*, perhaps to build a reputation for resolve.
	Policymakers can respond even when doing so undermines cherished policy priorities and can cause geopolitical ruptures	Supported. There is only one case – cyber was a major cause for Obama's flip from China-as-partner to China-as-competitor – but it is exceptional.
	Some responses are "intensifiers," which translate subjective perceptions into objective intensification of cyber conflict	Supported: larger budgets, new and larger cyber commands, looser restrictions, and more operations.

Several of these deeds might even be inherently credible signals, an index in Jervis terms.[194] For example, a U.S. governor declaring an emergency is an organic part of disaster response and not intended to signal to an adversary. This is also true, though to a lesser degree, for declaration of a "significant cyber event" or convening a Cyber Unified Coordination Group. This alone is an important finding for international relations.

Comparison with Other Approaches

To determine escalation in cyberspace, this method complements other approaches, uplifting evidence inadmissible or overlooked by other approaches. Inclusion of speeches, policies, and diplomatic responses, for example, allows better tracking of aggregate responses over time. This sheds light on, though does not solve, the mystery of the gap between international relations literature and the perceptions of apex policymakers. This method shows substantial escalation and demonstrates that Chinese cyber operations helped spark the American pivot to China-as-a-competitor, one of the most momentous diplomatic events of the century, a finding missed by other methods.

It is incontrovertible – but only part of the story – that cyber capabilities "can act as a less costly alternative to conflict because they are ambiguous, rarely break things, and don't kill people."[195] Far from there being a "Las Vegas effect" in which what happens in cyberspace, stays in cyberspace, it turns out that what happens in cyberspace ends up at the summit tables of presidents.

[194]Robert Jervis, *The Logic of Images in International Relations* (New York: Columbia University Press, 1970), p. 18.
[195]Erica D. Lonergan, "Cyber-Escalation Fallacy: What the War in Ukraine Reveals about State-Backed Hacking," *Foreign Affairs*, April 15, 2022, https://www.foreignaffairs.com/articles/russian-federation/2022-04-15/cyber-escalation-fallacy

Theoretical issues often raised in the literature do not feature in the words and deeds of policymakers.

- Over 40 percent (13 out of 31) of the incidents which most mattered to policymakers were perpetrated by non-states, generally overlooked as not relevant to international affairs.
- Another one third (10 of 31) were espionage (or criminal theft of information) despite many scholars considering espionage almost inherently non-escalatory, since every state does it. The U.S.-China example in particular shows the weakness of this assumption, as espionage can cause lasting geopolitical rifts.
- Policymakers responded not just to the impact of any single incident, but also the cumulative effects over time, which can be missed in the bilateral-counteraction method.
- Cyber operations can be covert and difficult to attribute, initially dampening escalation, but later (after repeated incidents over time) policymakers showed little doubt who was tormenting them.
- Nor is there any evidence of variance over time, as would be expected in an intelligence contest.

The comparison with cyber persistence theory is more complex. Though our evidence confirms its prediction that norms may not be meaningfully determined beforehand, we find no evidence for the core expectation of that theory, that more persistent cyber operations lead to lower levels of strategic interaction. Since the U.S. began persistent operations in 2018, policymaker's concerns have only become more intense. It is unclear by what mechanism any future doubling down on aggression might pacify the situation, rather than spiraling into more vivid incidents and angry policymakers.

Part 6.2. Alternative Explanations and Critiques

There are, of course, other possible explanations. Perhaps this methodology amplifies perceptions of escalation and misses de-escalation? Unlikely. There were no qualitatively meaningful responses over the 15 years of the baseline period, yet such responses were plentiful over the next 15, across nearly all lines of evidence and across a range of apex policymakers, from both parties. Strategies, policies, budgets, staffing, authorities, operations: none decreased; all increased steadily. This likewise rules out policymakers' words being all empty talk or signaling, as their words were consistent and closely matched their deeds across many administrations.

Obama's shift to China-as-competitor *preceded* broader geopolitical tensions, ruling out a second possible explanation: that perception is necessarily driven by broader geopolitics, not the cyber operations themselves.

A third possibility is less of an alternative explanation than a critique: do these words and deeds reflect "escalation," perhaps because objective criteria should trump the subjective or there was no break to actual violence. We disagree. But even accepting this criticism at face value, policymakers' words and deeds indicate a major shift in strategic interactions with nuclear armed rivals, which demands scholarly explanations. If the "subjective" label were stripped away from this paper, the actions of policymakers (especially the intensifiers) could all be considered objective evidence of escalation. And since it is apex policymakers who will be making decisions of peace and war; their past interpretations are important predictors of their future actions.

Part 6.3: Why Did Apex Policymaker Respond as They Did?

A range of objective and psychological factors seem to drive perception and response.

Policymakers seem to have valid worries about objective criteria cited in cybersecurity literature. According to research funded by the U.S. Department of Homeland Security, incidents reported each quarter have increased 650 percent since 2010. A typical firm is 3.7 times more likely to have had an incident since 2008, with median losses higher both overall and relative to a firm's revenue (over 15 times and nearly eight times higher, respectively, in constant dollars).[196] It is not irrational to be concerned.

Moreover, policymakers are not alone with their concerns. Surveys have found that 84 percent of C-suite leaders say their organization's focus on cybersecurity has increased compared with three years ago.[197] The index of cybersecurity, a sentiment analysis of key practitioners, increased nearly monotonically from a base of 1000 in 2011 to nearly 8000 in 2024.[198] Most importantly, policymaker's perceptions also match assessments from their intelligence agencies.[199] The closer to classified information, the more concerned experts seem to be, the opposite of the expectation if policymakers are simply wrong, over-reacting, or irrational.

Beyond that, we must surmise, about what is going inside the heads of policymakers. Based on their words and deeds, we have some initial, tentative suppositions.

Before an incident, being in a "constant state of near ambush,"[200] apex policymakers may be driven by a sense of strategic vulnerability. This is a complex mix of both objective factors (such as intelligence assessments about of adversary organizations and capabilities; known vulnerabilities

[196]Cyentia Institute, "Information Risk Insights Study 2025," https://www.cyentia.com/iris2025/
[197]EY, "Cyber Study: How the C-Suite Disconnect Is Leaving Organizations Exposed," 2025, https://www.ey.com/en_us/ciso/cybersecurity-study-c-suite-disconnect
[198]*Index of Cybersecurity*, https://wp.nyu.edu/awm1/
[199]For example, cyber has featured in annual threat assessments; see https://www.intelligence.gov/annual-threat-assessment.
[200]McDermott, "Emotional Dynamics of Cyber Conflict."

in critical infrastructure; and the impact of past failures, incidents and campaigns, magnified by geopolitical tensions) and subjective factors (including personal threat perception, vivid experiences of past incidents, a sense of vulnerability, uncertainty, loss of trust in technology, and both fear (a response to a specific, known threat) and anxiety (a response to a vague, systemic, or unknown threat)).[201]

During and after an incident, objective factors seem to drive much of the response: *what is the impact and what actions must we take to mitigate the incident and prevent cascading failure*? Subjective factors also have a role. Policymakers are certainly stressed and seem to fear specific impacts of disruption to critical infrastructure and be anxious about the many uncertainties. This is especially likely for espionage, for which actor, intent, and scope of the intrusion may not be known for weeks. Policymakers may be outraged as well when the incidents are vivid and the impact is personal (e.g., the Obama administration feeling "pissed off" over the OPM breach) or seen as a brazen affront (e.g., Russia's election interference).

During the *baseline period of strategic interaction*, policymaker's reactions seem to have been characterized by fear and anxiety, surprise, and stress. Surprise and fear together generate alarm, as evidenced by policymaker attention from 1998 onwards. Fear also leads people to be less risk-taking, to step back to better understand the situation, which may help explain policymaker's restraint in the baseline period. Policymakers may have experienced learned helplessness, after so many repeated, painful incidents when their traditional policy toolbox seemed useless.[202]

[201]As summarized in McDermott, "Emotional Dynamics of Cyber Conflict."
[202]Lyn Y. Abramson, Martin E. Seligman, and John D. Teasdale, "Learned Helplessness in Humans: Critique and Reformulation," *Journal of Abnormal Psychology* 87, no. 1 (1978): 49–74.

By the *subsequent period of strategic interaction*, from 2012 onwards, they may have felt psychological reactance, a need to reassert control no matter the cost[203] and a need to show resolve. For example, Obama's response to the Sony incident was *here and no further*: "[w]e cannot have a society in which some dictator someplace can start imposing censorship here in the United States." The fundamental attribution theorem may also apply: policymakers might seem to imply U.S. cyber campaigns are reasonable measures to improve global security, while adversaries are implacable and their operations malicious.

In this latter period, fear might have turned to anger, which leads people to be both more risk-seeking and more likely to blame others, instead of situational factors.[204] Policymakers may have felt a status deficit[205] or be operating in the domain of loss compared to adversaries,[206] which can drive an action bias,[207] the need to take control and make relative gains against tormentors. To reclaim agency and stop the bleeding, policymakers may have reached for intensifiers – new cyber commands, with more staff and higher budgets, with fewer constraint – to dictate the tempo and force the adversaries to react for a change.

Facing such intensifiers, rival apex policymakers may face a similar mix of objective and subjective drivers, leading them to approve their own intensifiers unleashed against the United

[203]Stephen A. Rains, "The Nature of Psychological Reactance Revisited: A Meta-Analytic Review of over Thirty Years of Research," *Human Communication Research* 39, no. 2 (2013): 150–173, https://doi.org/10.1111/hcre.12002.
[204]McDermott, "Emotional Dynamics of Cyber Conflict."
[205]Rose McDermott, *Political Psychology in International Relations* (Ann Arbor: University of Michigan Press, 2004).
[206]Levy, "Prospect Theory, Rational Choice, and International Relations."
[207]Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981).

States. This positive feedback would feed competition at ever-higher levels with few obvious or satisfying escapes.

Part 6.4: Lessons and Future Research

The lessons start with those for policymakers to better understand the situation they face. Rivals have not yet responded to a cyberattack with traditional military force. While policymakers clearly distinguish between responding with traditional weapons compared with other means, they make no distinction between responding *within* or *outside* of cyberspace.

Being virtual makes cyberspace no less existential, as cyber operations blossom into cyber crises which in turn drive geopolitical turmoil. Although cyber capabilities indeed have been used as accommodative signaling to de-escalate, there are more examples where they were perceived as a willingness to further escalate. Worse is yet to come. In an increasingly crisis-rich world, "states will increasingly feel angry, paranoid, trigger-happy, and vengeful, and they will turn to their militaries for salvation — a chaotic recipe, ripe for error, and potentially overwhelming any dampening effects of cyber capabilities."[208]

There are no easy escapes. Persistent engagement promises a never-ending series of tactical engagements between the cyber forces of nuclear armed rivals. Taking the fight to the enemy seems likely to push rival policymakers further into the domain of loss, fed by their own steady diet of vivid incidents, adding to their grievances and encouraging them to take even larger risks. Such dangerous situations require close political monitoring, not delegation and longer leashes.

[208]Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review* 3, no. 4 (2020): 30–53.

Policymakers should rather focus on resilience and shifting more advantages from offense to defense, so that there are fewer opportunities for vivid incidents.[209]

There is another set of lessons for those studying escalation in any domain, not just cyber. This method should be useful to study any competition in which there are few quantifiable objects about which to be objective. In such cases, who gets to decide if a particular incident is escalation or not? The answer from academics is not necessarily more objective than that of policymakers, their judgements about which incidents are more intense than another are still just judgments. If one measure of escalation is targeting of politically sensitive targets, for example, then assessments cannot ignore the sensitivities of politicians.

Escalation cannot be reduced to just rational, prior assessments of what actions a particular researcher thinks might be more intense than another. Any datasets coding for intensity should be considered tentative and later calibrated with the actual responses of policymakers. As Slovic, et al, have assessed, "human decision-making is often driven not by logical deliberation, but by heuristics, biases, and emotional responses that can distort perceptions of risk and reward, even in matters as consequential as war."[210] The field must respond to policymakers as the humans they are, not as paragons of rationality.

Future research design should accordingly complement objective approaches by investigating the words and deeds of policymakers, such as with interviews and mining memoirs, archives, and high-quality journalistic accounts. Additional research should more fully incorporate the full range

[209]Columbia University School of International and Public Affairs (SIPA), "Building a Defensible Cyberspace: New York Cyber Task Force," 2017, https://www.sipa.columbia.edu/global-research-impact/initiatives/cyber/nyctf/defensible-cyberspace

[210]Paul Slovic, Missy Peterson, Rose McDermott, Daniel R. Post, and Daniel Västfjäll, "When Our Minds Go Nuclear: Rethinking Nuclear Strategy through the Psychology of Risk and Decision-Making," *Texas National Security Review* 9, no. 3 (Summer 2026): 8–27, https://tnsr.org/2026/06/when-our-minds-go-nuclear-rethinking-nuclear-strategy-through-the-psychology-of-risk-and-decision-making/.

of political psychology, especially prospect theory and the roles of trust, uncertainty, and emotion. Subjective escalation methods will be increasingly critical as so many of America's key adversaries are personalist dictators: U.S. operations are escalatory if Xi Jinping and Vladimir Putin believe they are.[211]

Specifically for cyber, the perception of policymakers should also be at the core of research in related areas like coercion and offense-defense balance, which have similar gaps between scholars and policymakers. International relations researchers should no longer exclude non-state incidents or downplay the escalatory impact of espionage campaigns, as presidents have treated these as critical for years.

It is not merely a cliche that we live in an information age. Policymakers treat cyber issues as existential, prioritizing them over more traditional economic and security issues and responding with nearly every lever of power short of armed attack. If escalation is about perception, then it must be linked to political psychology, which tells researchers, "We have to observe and listen to people."[212] And the people, in this case, apex policymakers, are speaking very clearly indeed.

Acknowledgements: Will be re-added after peer review to avoid inclusion of any identifying material.

[211]Rose McDermott, "Psychology, Leaders, and New Deterrence Dilemmas," in *The Fragile Balance of Terror: Deterrence in the New Nuclear Age* (Ithaca, NY: Cornell University Press, 2023), pp. 39–62.
[212]Robert Jervis, *How Statesmen Think: The Psychology of International Politics* (Princeton, NJ: Princeton University Press, 2017), p. 5.