Allegations of U.S. Cyber Hegemony Complements China's Influence Campaign

to Weaken Global Confidence in the United States

Emilio Iasiello

ABSTRACT

The People's Republic of China (PRC) has engaged in an aggressive media campaign, using classified data leaks exposing controversial United States (U.S.) cyber activities to paint it as a cyber hegemon. This effort has dovetailed with other influence operations in an effort to frame the U.S. as an untrustworthy global partner motivated by its own self-interests ahead of the global community. The U.S. Department of State released a recent report on these activities, correctly concluding that they have had questionable successes. However, the PRC is using these campaigns not so much as to supplant the U.S. as a global leader, but rather to keep it in check by raising questions in the minds of those nations not already bound to the U.S. to not blindly follow Washington's lead. The PRC seeks to capitalize on this to press forward on core political and economic issues, which if achieved, could put the PRC closer to its goals as an influencing global leader.

Keywords: *Cyber, China, Cyber Hegemony, Influence Campaign*

INTRODUCTION

Over the past year, the PRC has engaged in an antagonistic media campaign criticizing U.S. global cyber activities as hegemonic, designed to exert undue influence and dominance over the Internet domain to advance its interests as the world's preeminent cyber leader. Via its state-controlled online media channels, the PRC has leveraged classified data leaks and the U.S.'s "defend-forward" cyber strategy to buttress the narrative describing the U.S. as a hypocritical nation, driven solely

Emilio Iasiello has more than twenty years of experience as a strategic cyber intelligence analyst, supporting U.S. government civilian and military intelligence organizations, as well as the private sector. He has delivered cyber threat presentations to domestic and international audiences and has published extensively in such peer-reviewed journals as *Parameters*, the *Journal of Strategic Security*, the *Georgetown Journal of International Affairs*, and West Point's *The Cyber Defense Review*, among others.

by self-interest, and guilty of the very activities it attributes to other nations. This media blitz dovetails with other PRC information campaigns that seek to discredit the U.S. with respect to other issues, such as military support for Ukraine and Israel, thereby framing Washington as a government that pervasively interferes in other state's affairs. This aggressive position, driven by Xi Jinping, stands in stark contrast to the more passive approach under Hu Jintao and the peaceful development strategy aimed to mitigate conflict as the PRC achieved its objectives gradually. Xi no doubt perceives a U.S. that is weakened by internal political division,[1] back-seated to a secondary role in world affairs, and less able to drive foreign policy. To capitalize on this, Xi appears to envision more maneuverability on the world stage to pursue the PRC's global aspirations.

THE PRC KEEPS LIGHT ON QUESTIONABLE U.S. CYBER ACTIVITIES

In response to allegations from cybersecurity companies and foreign governments over its pervasive offensive cyber operations, the PRC has issued official denials, citing its own victimization at the hands of malicious attackers.[2] In response to accusations from victims, the PRC stubbornly demands proof of such claims.[3] It was only after repeated U.S. accusations citing the PRC as a prominent cyber threat in its unclassified threat assessments, coupled with the 2020 Chinese cybersecurity company Qihoo 360 attributing hostile cyber activity since 2008 to the U.S. Central Intelligence Agency (CIA),[4] that the PRC shifted its tack. This 2020 shift by the PRC upgraded its passive "deny, deny, deny" strategy with a more offensive attack, seeking to expose U.S. cyber malfeasances and neutralize U.S. success in leveraging the U.S. cybersecurity community to publish and disseminate findings of a foreign government's cyber operations.

The 2020 Qihoo 360 report marks the beginning of PRC efforts to expose U.S. cyber surveillance and

operational activities, and thereby paint the U.S. as the premier cyber threat to the global community, letting the world know that the PRC too is capable of tracking highly sophisticated threat actors operating in cyberspace. Several state-controlled and/or influenced PRC media sources such as the *Global Times*, *South China Morning Post*, and *China Military* since 2020 have published accusations in efforts to "name and shame" alleged U.S. cyber campaigns in an attempt to expose the U.S. and otherwise shift attention. Notable articles have highlighted incidents where the U.S. has allegedly conducted the types of activity that it has accused the PRC of doing.

Themes	Chinese Media "Naming and Shaming" Campaigns
Recruiting Insiders to Support Cyberspying	In November 2023, the PRC's Ministry of State Security (MSS) reported an investigation involving the recruitment of a Chinese software developer that provided "technical services" to a foreign spy agency. The spy agency had corrupted the software to conduct cyberattacks and steal information from several of Chinese defense and high-tech organizations, according to the *Global Times*.[5] While the U.S. was not specifically named in the article, the innuendo was that the expertise and sophistication was telltale.
Internet Governance	In November 2023, the *Global Times* took the lead in condemning the U.S. as a cyber hegemon, in stark contrast the the PRC's vision of a shared future in cyberspace underpinned by joint contribution, shared benefits, and collective resolution of security challenges,[6] and otherwise condemning perceived U.S. hegemonic practices of global surveillance, building cyber arsenals, coercing governments to thwart PRC telecommunications, and massive data theft.[7]
Huawei Enabling Spying	A September 2023 article on the English-language website of the *China News Service* reported on the PRC's Ministry of State Security's (MSS) revelation of U.S. infiltration of Huawei via the NSA's Tailored Access Operations (TAO) dating back to 2009. The MSS claimed TAO carried out thousands of attacks targeting the PRC, stealing extensive high-value data.[8] This release countered U.S. and other government outcries against Huawei as a state enabler of PRC cyber operations.
Targeting Education	In September 2023, both the *South China Morning Post* and the *Global Times* published articles identifying the NSA of cyber surveillance and data theft against Northwestern Polytechnical University, claiming a PRC team found "thousands of network devices" infected by NSA spyware.[9]
High-Value Targets	In August 2023, the *Global Times* reported a joint public-private investigation that revealed U.S. cyber military team cyber espionage attacks against the Wuhan Earthquake Monitoring Center, which monitors earthquake activity. Per a leading Chinese cybersecurity company's analysis, the attacks sought to steal geological data to better understand battlefield terrain.
Global Surveillance	In February 2022, Chinese cybersecurity company Pangu Lab identified that for more than a decade the NSA had conducted global surveillance against 45 countries and regions. This marked the first time a Chinese company publicly shared technical evidence of a state-orchestrated cyber attack by alleged U.S. cyber actors.[12] It also strongly suggested that the U.S. was the world's most prominent cyber threat actor conducting global surveillance against friendly and adversarial nations alike. Several Chinese media sources echoed a report by a cybersecurity company in Burma that detailed TAO efforts to remotely obtain more than 97 billion Internet data records along with 124 billion phone records in 30 days.[13] While never made publicly available, references to this report casts the U.S. as a global spying and cyber thief.

Table 1. Cyber Themes Highlighted in Chinese Media Campaigns.

The PRC's assertive campaign benefits from the fact that governments need not prove attribution so much as to simply claim a government is responsible for a cyber attack. Unlike conventional crimes like terrorism or nuclear arms development, governments may be hesitant to "show their work" when it comes to cyber attack attribution, which can compromise sensitive collection platforms and mechanisms. This may be one of the reasons why cyber security companies actively produce APT reports and are more willing to attribute activity to a nation state, and certainly calls into question if these companies are collaborating or at least taking

direction from their host governments. Among leading cybersecurity companies, Kaspersky is one of the few that avoids attributing cyber attacks to specific governments, instead preferring the more generic classification of "state actor." As Eugene Kaspersky said in an interview, "we never do attribution."[14]

Under Xi, the PRC adopts a more aggressive stance as to its position in the world and it combats negative perceptions that it is a nefarious cyber actor. The PRC no doubt views Washington's constant harassment of its cyber activities as hypocritical, and counters with calling out the U.S. for similar activities. What has undoubtedly helped fuel the PRC's message are the Edward Snowden leaks and the Shadow Brokers, a murky group that reinforced suspicions that the U.S. cyberspace mischief exceeds that of the PRC. The 2013 Snowden treasure trove revealed highly sensitive U.S. technologies and exposed the expanse and breadth of U.S. surveillance capabilities. Many already suspected the U.S.'s formidable resources; the Snowden leaks removed all doubt. Documentaries such as *CitizenFour* and films like *Snowden* kept the image of the U.S. as a global surveillance ogre, and augmented the PRC's campaign to chip away at the U.S. image as a democratic champion and frame us more as a cyber hegemon protecting our superiority in cyberspace, superiority that has steadily declined as more governments embraced and implemented technology to support their own national interests.

The U.S. had not yet recovered from the Snowden disclosures when the mysterious Shadow Brokers group leaked the tools allegedly used by the NSA, exposing tools and vulnerabilities used to break into routers, platforms like Microsoft Windows, Linux mail servers, and even the SWIFT banking network.[15] While no definitive proof tied this group to the NSA, in early 2017 a former NSA contractor was arrested for stealing 75% of TAO's hacking tools, strengthening the assumption that the Shadow Brokers included at least one ex-NSA operative.[16] After the 2017 incident, the Shadow Brokers never resurfaced. The leak was very likely intended to embarrass the U.S. and otherwise thwart future activities. More damning, any doubt about U.S. global spying was removed. Washington could no longer deny its formidable spying endeavors, and now friendly nations like France[17] and Germany[18] were protesting against the U.S. for doing the same thing against them. For the leading democratic nation, such activities beyond the guise of "national security" are difficult to spin.

For most of 2023, the Chinese press has pushed the "U.S. cyber hegemon" narrative, which also conincided with PRC's perception of U.S. weakness on the global stage. *The Global Times*, *China Military,* and *China Daily* and PRC-allied news sources like Iran's *Tasnim News Agency*,[19] ran articles in 2023 condemning the U.S. as a cyber hegemon bully, which was imperiling rather than strengthening for global security. The articles reported continued development of U.S. cyber military apparatus, to include deployed hunt-forward teams, CIA's hacking activities, and U.S. reluctance for embracing multilateral Internet governance.[20]

Another PRC accusation is the U.S.'s willingness to levy cyber sanctions in coercing the global community. The *Global Times* reported the U.S. sanctions and places companies on export

control lists to protect its military and cyber hegemony under pretence of national security, obfuscating its true purpose – to thwart PRC competition and growth.[21] Supporting reasons for such sanctions included "human rights violations" and "invasion of privacy" concerns – two subjects the PRC would counter in subsequent press articles by showing where the U.S. was guilty of the very same allegations. The PRC is fervently committed to highlighting hypocracies and otherwise tarnishing the U.S.'s reputation as a beacon of democratic principles.

This has been facilitated by the political polarization in the U.S., particularly as to state-orchestrated surveillance, a charge frequently levied against the PRC and other authoritarian regimes by Western governments. Indeed, even organizations such as the American Civil Liberties Union acknowledges rampant overreach by surveillance authorities, particularly from the NSA.[22] Capitalizing on internal U.S. controversies, the *Global Times* quickly spearheaded a campaign to show hypocritical policies the U.S. has engaged in with its own citizens, depicting a surveillance state driven by FBI, CIA, and even Immigration and Customs Enforcement,[23] thereby exposing U.S. hypocrisy, especially over human rights issues.[24]

THE PRC'S "FREE" MEDIA AGAINST THE U.S.

Throughout Xi's tenure, and especially over the past eighteen months, the PRC has become increasingly combative toward critics that singled out the PRC for cyber offenses. The PRC has ramped up efforts to smear the U.S. not just from a cyber perspective, but in other areas as well, as evidenced by its media voraciously publishing negative news about the U.S. (and other Western governments that threaten the PRC) on topics that include poverty, pollution, oligarch control of politics, and racial tensions.[25] The increasing tempo of this negative press prompted the U.S. Department of State to report on the PRC's broader disinformation campaigns designed to shape the global information environment to favor PRC interests,[26] noting these campaigns include propaganda, censorship, promoting digital authoritarianism, and exploiting international partnerships, in short, tactics the Chinese press claim against the U.S.[27]

What is certainly noticeable is the PRC's shift in posture with respect to how it's been pursuing its goals, moving from passive "peaceful development" under Hu Jintao to a more aggressive and ambitious "national rejuvenation" strategy role under Xi's stewardship.[28] A critical part of this shift has been the PRC's willingness to go after its detractors and critics that seek to hurt the PRC's image or impede their global social, cultural, and economic gains. It also has required the PRC to take advantage of situations where their principal adversary – the U.S. – has been at its weakest. Over the past several years, the U.S. has steadily declined as an international presence, in part due to internal (border issues, race and gender issues, etc.) and external crises (Ukraine war, Israel-Palestine conflict), which have stretched its standing and, to a certain extent, its capabilities.[29]

The PRC flags key issues in an attempt to cast the U.S. as a "flawed democracy." Indeed, the 2022 *Democracy Index* report by the Economic Intelligence Unit found that the U.S. ranked

26th of 167 countries when measuring elections, government, and civil liberties, among other categories.[30] Unsurprisingly, this has been a theme in the PRC's government communications and one the Chinese media has contributed to significantly, exploiting those issues where the U.S. has been traditionally strong, (e.g., human rights, standing by its word on the global stage, etc.) to create fissures in the U.S.'s image as the leader of the free world, a position it unofficially has enjoyed since the Cold War.[31] Four recent issues that underscore the PRC's discrediting efforts include the botched Afghan withdrawal; perceptions of U.S. censorship of social media; perceptions of targeting political opponents; and allegations of U.S. spying.

Themes	Chinese Media "Naming and Shaming" Campaigns
Afghan Withdrawal	Though most Americans favored te U.S. withdrawl from Afghanistan, the hasty manner in which it occurred[32] was perceived in the European press as a U.S. failing,[33] leaving Americans behind, resulting in the death of 13 U.S. Marines and reportedly failing to consult or coordinate with allies.[34] In short, it was viewed as a blunder by both domestic and international audiences alike, as corroborated by a Department of State report released in 2023.[35] PRC media exploited this to cast the U.S.as an unreliable partner and one that will put its own interests first despite its asserted commitments in an obvious effort to convince Taiwan to not rely on U.S. help as tweeted bythe *Global Time*s editor on social media.[36]
U.S. Censorship of Social Media	The PRC also exploited reported instances of U.S. government pressuring social media companies to censor and/or restrict to the U.S. public, including COVID-related issues and the Hunter Biden laptop, citing a lawsuit accusing the U.S. government of unconstitutional censorship.[37] Despite the fact that the U.S. Supreme Court sided with the Adminsistation, first on an interim basis in September 2023, and ultimately in a 6-3 final decision in June of 2024, this did not prevent the PRC media from trying to exploit U.S. policy regarding authoritarian surveillance and censorship, claiming it to be hypocritical, and running news articles calling the U.S. a "surveillance empire" and an "empire of lies."[38]
Targeting Political Opponents	U.S. politics, according to some factions, is increasingly strained. When government agencies take actions against members of the opposing political party, it is reminiscient of authoritarian regimes that seek to remain in power. Indeed, Mike Pompeo, Secretary of State in the Trump Administration in 2022 went so far as to accuse the Biden Administration of leveraging government agencies like the FBI and Department of Justice against a political rival in the upcoming 2024 U.S. presidential election.[39] A March 2023 poll found that nearly two-thirds of those responding thought the FBI had become politically weaponized.[40] This was not the first time an Administration was accused of such an abuse of power. In 2017, the Internal Revenue Service was accused of delaying approvals of nonprofit status for conservative groups engaged in public education and voter mobilization.[41] For each of these instances, the Chinese press has feverishly seized the narrative[42] in the PRC's effort to accentuate U.S. hypocrisy and deem the U.S.'s "politics of retaliation" as counter to the even-handed principles of democratic governance.[43]
U.S. Spying	*The Global Times*, exploiting a *Wall Street Journal* (WSJ) article that detailed the CIA's spying activities against the PRC, charged the U.S. with hypocrisy when we accuse the PRC of its relentless spying.[44] The WSJ article recounted a CIA spying failure a decade ago in the PRC when U.S. spies allegedly were caught, thereby setting back U.S. intelligence work.[45] The *Japan Times* reported the CIA as having doubled its spending against the PRC and increased its own surveillance against Chinese companies.[46] This article also reported the CIA as investing heavily into intelligence collection on Chinese companies developing advanced technologies like Artificial Intelligence, information the U.S. had not typically collected in the past.[47] From this, the PRC crafted narratives to promote its own anti-espionage activities as dealing costly blows to U.S. spy agencies efforts while claiming the gap between our two intelligence services has greatly narrowed.[48]

Table 2. Geopolitical Themes Highlighted in PRC Media Campaigns.

IS CHINA'S MEDIA CAMPAIGN WORKING?

Media attacks against U.S. cyber policies complement the PRC's overall efforts to enhance perceptions of U.S. weakness and untrustworthiness and further tarnish the U.S. brand. And while we cannot accurately correlate Chinese media themes' and actual global perceptions of the U.S., the PRC's media campaigns are very real, as are these perceptions. Two prominent

polling organizations found that the U.S. has lost credibility over the past few years both internally and externally. In 2022, a Gallup poll found that the U.S. earned the least confidence from its citizens of any G7 member country besides the United Kingdom, falling to 40% in 2021 and 31% in 2022.[49] Pew Research found that of 24 countries surveyed (mostly Western), the majority found the U.S. better than the PRC, however, they also overwhelmingly believed that the U.S. constantly interfered in other countries' affairs.[50] The same survey also confirmed positive views of the U.S. as compared to the PRC in terms of military strength, entertainment, high education, standards of living, and personal freedoms but noted on economics and technology, the PRC and the U.S. drew nearly even, suggesting areas that the PRC could strengthen its engagement with international partners. It would not be surprising to see Beijing increase its efforts in these areas over the next twelve months in an effort to gain competitive advantage over the U.S.

Still, despite the PRC's prolific production of content, the Department of State report correctly concluded that PRC-driven information campaigns have yielded mixed results, which is supported by the two surveys cited above, and many in the global community still favor the U.S. over the PRC. Yet, governments need not like or agree with a country to do business with it. Case and point: the first 11 months of 2023 saw PRC exports of USD $458.5 billion to the European Union, while corresponding imports totalled USD $357.8 billion.[51] Thus, even with the majority of European states not liking the PRC's policies, a European Council on Foreign Relations reported that most of the continent views the PRC as a "necessary trade partner" and not an adversary.[52] And Europe is not alone, the PRC is the top trading partner for more than 120 countries, to include developing nations in Latin America, Africa, and Asia.[53]

This economic reality matters in framing the PRC's strategic priorities like Taiwan, and some EU countries may well recuse themselves from a cross-strait conflict or provide little substantive aid to Taiwan. The PRC does not need Europe as a military ally as much as it needs Europe to embrace economic advantage over a geopolitical incident that little impacts their continent, and also to avoid overtures to form coalitions against the PRC's interests. And French President Macron, in an April 2023 visit to the PRC, urged Europe to reduce dependence on the U.S., saying that France should not take its cues from the U.S. on issues like Taiwan and be dragged into such unnecessary conflicts.[54]

And this may very well be the crux of the PRC's media attacks. By steadily trying to chip away at the U.S.'s credibility, tarnishing our image as a democratic paragon, and exposing hypocrisies, the PRC may be more focused on sidelining foreign governments rather than creating new allies. It only needs to instill enough doubt about the U.S. to weaken resolve, soften stances, and otherwise avoid governmental barriers on issues the PRC deems vital to its interests such as Taiwan, becoming the world's largest economy, and being a leader and integrator of emerging technologies. Uncoincidentally, their media attacks against the U.S. on cyber-related matters ties directly to each of these core objectives.

CONCLUSION

The U.S. Department of State's report confirms the PRC's efforts to shape the global information environment appear less about spinning a faulty narrative than capitalizing on, even exaggerating, existing discord and distrust. But to claim the PRC is fabricating discord is conspiciously disingenuous and thus, not even credible. That the PRC's campaigns have become increasingly voluminous and pervasive strongly suggests that the PRC perceives the U.S. as vulnerable on the world stage.

The PRC's media attacks bend more toward influence than incitement, suggesting a PRC nuanced objective. The themes are consistent regardless of the topic and center on one theme – the U.S. is no longer essential in today's geopolitical environment, or anywhere near as essential as it was in the past, going back to World War II. The U.S. no longer embraces the same democratic principles it once championed, is increasingly guilty of demanding "do as I say, not as I do," and has an increasingly tarnished public image. At World War II's end, the U.S.'s role internationally was one of global leadership, fueled by the world's strongest economy and a built-up military.[55] But in the past 20 years, the U.S. gradually retreated from that position due to a failure to take decisive action or otherwise achieve U.S. policy goals responsive to international incidents, with some leaders blaming one or another administration.[56]

Fast forward to today, and it's apparent that the United States has continued this trend, suffering several foreign policy missteps and inconsistencies, especially with the two largest elephants in the room (Ukraine war, Palestine conflict) and the disparity in the support the U.S. has provided Ukraine and Israel. This is disconcerting given that in an October 2023 speech, President Biden directly linked both of their outcomes to the security of the U.S.[57] Adding insult to injury are the governments of Saudi Arabia, China, and Iran blatantly disrespecting the U.S. on the global stage by ignoring U.S. overtures for executive-to-executive engagement over oil production, stalling on restarting military-to-military communication, or using returned millions in frozen funds without restriction.[58] This further perpetuates the image that the U.S.'s influence may not be as what it once was.

Chinese media attacks against the U.S. on cyber-related issues have potential greater ramifications than just solely discrediting our government. The global community has failed to make any significant progress on codifying cyber norms of state behavior in cyberspace as well as other key areas like state cyber sovereignty. Viewed from this perspective, this Chinese media campaign can be seen as a vehicle to influence those governments in the United Nations to align themselves with either the PRC or Russian preference for a government-led approach to Internet governance as opposed to the West's multi-stakeholder model.[59] At best, the PRC gains support in the UN. At worst, continued failure to agree to a consensus perpetuates the status quo where nation states continue to act with impunity in cyberspace with minimal repercussion.

What seems clear from what is not classified is that the U.S. has not exercised a strong strategy against the PRC's cyber malfeasances, which suggests greater concern for the potential benefits of a relationship and avoiding conflict. Washington must endeavor to maintain a productive working relationship, even as the two remain fierce competitors and borderline adversaries. And the PRC understands that its active cyber apparatus notwithstanding, it cannot match the U.S. in capability, sophistication, and reach. So, instead of meeting it head on, it will leverage demonstrations of U.S. cyber power to buttress assertions that Washington's cyber program overreaches with its hunt-forward operations and overly aggressive in efforts to govern the Internet.

Xi's current strategy with the media campaign does not appear to seek to supplant the U.S. as the reigning global cyber power, but rather, to keep it in check. It does that best by publicizing its cyber activities against the PRC to depict the U.S. as an irresponsible state cyber actor. The strategy may or may not succeed and may be better observed in the UN as Internet governance issues play out. As the Department of State report confirms, the PRC's focus is more on influencing the greater information space, and less on showing it has bigger cyber muscles than Washington. Because true power comes not from disrupting or destroying infrastructures but by setting the standards and norms in the domain where such battles are and will be fought.

DISCLAIMER

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the U.S. Government.

NOTES

1. For more on China's disinformation campaign to influence our elections and amplify divisive U.S. political issues see: Jeremy B. Merrill, Aaron Schaffer, and Naomi Nix, "A Firehouse of Antisemitic Disinformation from China Pointing at Two Republication Legislators," (October 10, 2024). *The Washington Post*, https://www.washingtonpost.com/technology/2024/10/10/us-elections-china-influence-x/.
2. Jim Randle, "China Says it Is Victim of Cyber Attacks; Not Victim," (March 19, 2013). *Voice of America News*, www.voanews.com/a/china-says-it-is-victim-of-cyberattacks-not-perpetrator/1624718.html; A Martinez and Emily Feng, "China Denies Cyberattack Accusations; And Says It Too Is A Victim of Hacking," (July 20, 2021). *NPR*, https://www.npr.org/2021/07/20/1018271511/china-denies-cyberattack-accusations-and-says-it-too-is-a-victim-of-hacking.
3. Dustin Waltz and Josh Chin, "U.S. Believes It Doesn't Need to Show Proof Huawei is a Spy Threat," (January 23, 2009). *The Wall Street Journal*, https://www.wsj.com/articles/u-s-believes-it-doesnt-need-to-show-proof-huawei-is-a-spy-threat-11548288297.
4. Qihoo 360, "APT-C-39," (March 2020), http://blogs.360.cn/post/APT-C-39_CIA_EN.html; Pierluigi Paganini "CIA Hacking Unit APT-C-39 Hit China Since 2008," (March 2020). *Security Affairs*, https://securityaffairs.co/98885/apt/cia-hacking-china.html.
5. *The Global Times*, "Foreign Spy Conducts Cyberattacks Against China's Defense, High-Tech Firm by Recruiting Chinese Developer," (November 27, 2023). https://www.globaltimes.cn/page/202311/1302547.shtml.
6. *The Global Times*, "Cyber Governance Should Not Be Controlled by Group Politics, Zero Sum Thinking," (November 8, 2023). https://www.globaltimes.cn/page/202311/1301441.shtml.
7. *The Global Times*, "Playing 'A Thief Crying Stop Thief' Trick, U.S. Only Wants Permanent Cyber Hegemony," (September 20, 2023). https://www.globaltimes.cn/page/202309/1298564.shtml.
8. Li Yan, ed., "China's Ministry of State Security Reveals U.S. infiltration of Huawei Traced Back to 2009," (September 20, 2023). Ecns.cn, http://ecns.cn/news/politics/2023-09-20/detail-ihctfqzx3360335.shtml.
9. William Zheng, "Beijing Says It Uncovered US National Security Agency Operatives Behind Cyberattack on Chinese University," (September 14, 2023). *SCMP.com*, https://www.scmp.com/news/china/politics/article/3234492/beijing-says-it-uncovered-us-national-security-agency-operatives-behind-cyberattack-chinese; Yuan Hong, "Identity of NSA Hacker Behind Cyberattack on China's Leading Aviation University Identified; to Be Disclosed in Due Course: Source," (September 14, 2023). *The Global Times*, https://www.globaltimes.cn/page/202309/1298164.shtml.
10. Yuan Hong, "Exclusive: China Identifies the Culprits Behind Cyberattack on Wuhan Earthquake Monitoring Center, A Secretive U.S. Global Reconnaissance System to Be Exposed," (August 14. 2023). *The Global Times*, https://www.globaltimes.cn/page/202308/1296226.shtml.
11. Yuan Hong, "Exclusive: Hackers Behind Cyberattack on Wuhan Earthquake Monitoring Center Aims at Stealing Geological Data: Top Cybersecurity Expert," (August 2, 2023). *The Global Times*, https://www.globaltimes.cn/page/202308/1295511.shtml.
12. Cao Siqi, "Exclusive: Evidence of U.S. Monitoring 45 Countries, Regions Exposed by Chinese Security Experts for the First Time," (February 23, 2022). *The Global Times*, https://www.globaltimes.cn/page/202202/1252952.shtml.
13. Qian Gong, "U.S.: Top Threat to Global Security," (September 22, 2022). *STDaily.com*, Google Translation to English, https://www.stdaily.com/English/BusinessNews/202209/c5f6006a75d0461la8e0f187f0cc8946.shtml; *China Daily*, "U.S. Hackers Extend Malicious Cyber Operations Around the World," (July 1, 2022). https://global.chinadaily.com.cn/a/202207/01/WS62be9236a310fd2b29e69d8c.html; *China Global Television Network (CGTN)*, "Operation Black Hand: U.S. Is the Primary Threat to Global Cyber Security,"(June 16, 2022). *CGTN.com,* https://news.cgtn.com/news/2022-06-16/Operation-Black-Hand-U-S-the-primary-threat-to-global-cyber-security-1aAC9I6xDu8/index.html.
14. BN Americas, "Eugene Kaspersky: 'We work with governments, not for them,' " (November 7, 2018). *BN Americas*, Chile', Interview with Eugene Kaspersky, https://www.bnamericas.com/en/interviews/eugene-kaspersky-we-work-with-governments-not-for-them--.
15. Bruce Schneier, "Who Are the Shadow Brokers?" (May 23, 2017). *The Atlantic*, https:// www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.
16. Dan Goodin, "Former NSA Contractor May Have Stolen 75% of TAO's Elite Hacking Tools," (February 6, 2017). *Ars Technic*a, https://arstechnica.com/tech-policy/2017/02/former-nsa-contractor-may-have-stolen-75-of-taos-elite-hacking-tools/.

NOTES

17. John Irish and Elizabeth Pineau, "Obama Reassures France After 'Unacceptable' NSA Spying," (June 24, 2017). *Reuters*, https://www.reuters.com/article/us-france-wikileaks-idUSKBN0P32EM20150623/.
18. *Reuters*, "U.S. Spied on Merkel and Other Europeans Through Danish Cables – Broadcaster DR," (May 31, 2021). *Reuters*, Copenhagen, https://www.reuters.com/world/europe/us-security-agency-spied-merkel-other-top-european-officials-through-danish-2021-05-30/.
19. *Tasnim New Agency,* "China Says US Seeks Cyber Hegemony," (April 8, 2023). *Tasnim News Agency*, Tehran, https://www.tasnimnews.com/en/news/2023/04/08/2877120/china-says-us-seeks-cyber-hegemony
20. Wang Qiang, "U.S. Eager to Seek Cyber Military Hegemony," (May 5, 2023). *China Military,* http://eng.chinamil.com.cn/OPINIONS_209196/Opinions_209197/16222055.html; Zhou Ningan, "Hacking Empire's Cyberspace Hegemony Endangers Global Security," (May 9, 2023). *China Military*, http://eng.chinamil.com.cn/WORLD_209198/WorldMilitaryAnalysis/16223609.html; *China Daily*, "Cyberspace Shouldn't Be a New Battlefield," (July 25, 2023). https://www.chinadaily.com.cn/a/202307/25/WS64bfb5b2a31035260b8186d2.html; Zhou Jin, "Beijing Speaks Out Against U.S.' Cyber Deployments," (August 10, 2023). *China Daily,* https://www.chinadaily.com.cn/a/202308/10/WS64d4ed9da31035260b818b6c3.html.
21. Global Times Staff Reporters, "Bullying Empire: How the U.S. Tries to Rule World's Internet Through Sanctions, China Slander Campaigns," (June 15, 2023). *The Global Times*, https://www.globaltimes.cn/page/202306/1292661.shtml.
22. Sarah Taitz, "Five Things to Know about NSA Mass Surveillance and the Coming Fight in Congress," (April 11, 2023). *American Civil Liberties Union*, https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress.
23. Xin Ping, "Life in the U.S. 'Empire of Surveillance': Trapped in a Dragnet," (August 12, 2022). *The Global Times*, https://www.globaltimes.cn/page/202208/1272851.shtml.
24. Tang Lan, "Surveillance Empire: Unrestricted Eavesdropping on Allies, Citizens Exposes Hypocrisy of American Human Rights," (May 25, 2023). *The Global Times*, https://www.globaltimes.cn/page/202305/1291394.shtml.
25. Hwang Chun-mei and Gu Ting for RFA Mandarin, "Chinese State Media is Pumping Out Bad News About U.S., Britain," (July 16, 2023). *Radio Free Asia*, https://www.rfa.org/english/news/china/china-bad-news-07112023142511.html.
26. United States Department of State, "How the People's Republic of China Seeks to Reshape the Global Information Environment," (September 28, 2023). Global Engagement Center Special Report, //www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/.
27. The People's Republic of China Ministry of Foreign Affairs, "Foreign Ministry Spokesperson's Remarks on the U.S. State Department's Report Targeting China," (September 30, 2023). *Ministry of Foreign Affairs*, https://www.mfa.gov.cn/eng/xwfw_665399/s2510_665401/2535_665405/202309/t20230930_11154141.html.
28. The People's Republic of China, "China's Peaceful Development,"(September 2011). Government of PRC, https://english.www.gov.cn/archive/white_paper/2014/09/09/content_281474986284646.htm; Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," (October 18, 2017). Remarks, Chinese Communist Party Conference, http://xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf.
29. Kathryn Levantovscaia, "Overstretched and Undersupplied: Can the US Afford its Global Security Blanket?" (January 5, 2024). *The Atlantic Council*, https://www.atlanticcouncil.org/blogs/new-atlanticist/overstretched-and-undersupplied-can-the-us-afford-its-global-security-blanket/; *Time Magazine Online*, "Is the U.S. Military Stretched Too Thin?"(original post August 23, 2003). Blog. https://content.time.com/time/nation/article/0,8599,477917,00.html
30. David Myers, "U.S. Remains a Flawed Democracy in Annual Rankings," (February 14, 2022). *The Fulcrum*, https://thefulcrum.us/big-picture/Leveraging-big-ideas/flawed-democracy.
31. *Encyclopedia of American Foreign Relations*, "Exceptionalism: The Leader of the Free World," (accessed May 1, 2024). https://www.americanforeignrelations.com/E-N/Exceptionalism-The-leader-of-the-free-world.html.
32. *United States Department of State,* "After Action Review of Afghanistan: January 2020-August 2021,"(March 2022), Report, https://www.state.gov/wp-content/uploads/2023/06/State-AAR-AFG.pdf.
33. "Allies Round on US After Afghanistan Withdrawal," (August 16, 2021). *France24 News Online*, https://www.france24.com/en/live-news/20210816-allies-round-on-us-over-afghanistan-debacle.
34. "Allies Round on US After Afghanistan Withdrawal."
35. *United States Department of State*, "After Action Review of Afghanistan: January 2020-August 2021,"(March 2022), Report, https://www.state.gov/wp-content/uploads/2023/06/State-AAR-AFG.pdf.

NOTES

36. Hu Xijin, *Global Times Editor*, China: Twitter Account Post, (August 16, 2021). https://twitter.com/HuXijin_GT/status/1427268690835705860.
37. Gabe Kaminsky, "Top Republicans Throw Support Behind Major Biden Censorship Lawsuit by Conservative Media," (December 11, 2023). *Washington Examiner*, https://www.washingtonexaminer.com/news/house/republicans-support-biden-censorship-lawsuit-gdi-newsguard.
38. Tang Lan, "Surveillance Empire: Unrestricted Eavesdropping on Allies, Citizens Exposes Hypocrisy of American Human Rights," (May 25, 2023). China: *The Global Times*, https://www.globaltimes.cn/page/202305/1291394.shtml; *China Daily*, "U.S. Attempts to Deceive World With Its Empire of Lies," (March 31, 2022), https://global.chinadaily.com.cn/a/202203/31/WS6244fc67a310fd2b29e5446b.html.
39. Michael R. Pompeo, "FBI Weaponized by Biden Justice Department in Campaign Against Trump," (August 12, 2022). *Fox News*, https://www.foxnews.com/opinion/fbi-weaponized-biden-justice-department-campaign-trump.
40. Anugrah Kumar, "Nearly Two Thirds of Voters Think FBI Has Been Politically Weaponized, Poll Suggests," (March 13, 2023). *Congresswoman Harriet Hageman's Website*, https://hageman.house.gov/media/in-the-news/nearly-two-thirds-voters-think-fbi-has-been-politically-weaponized-poll-suggests.
41. Bradley A. Smith, "A Lesson on the Abuse of Power By Obama and His Senate Allies," (October 10, 2017). *The Hill*, https://thehill.com/opinion/white-house/354680-a-lesson-on-abuse-of-power-by-obama-and-his-senate-allies/.
42. Jeremy B. Merrill, et. al., "A Firehouse of Antisemitic Disinformation from China Pointing at Two Republication Legislators."
43. Global Times Staff Reproters, "U.S. Falls Further into 'Politics of Retaliation' Amid Biden's Garage-Gate," (January 13, 2023). China: *The Global Times*, https://www.globaltimes.cn/page/202301/1283783.shtml.
44. Global Times, "Why is the CIA Openly Discussing Its Misdeeds Against China?" (December 27, 2023). Editorial, China: *The Global Times*, https:// www.globaltimes.cn/page/202312/1304439.shtml.
45. Warren P. Strobel, "American Spies Confront a New, Formidable China," (December 26, 2023). *The Wall Street Journal*, https://www.wsj.com/politics/national-security/american-spies-confront-a-new-formidable-china-5c384370.
46. Edward Wong, Julian E. Barnes, Muyi Xiao, and Chris Buckley, "Chinese Spy Agency Rising to Challenge the CIA," (December 28, 2023). *The Japan Times*, https://www.japantimes.co.jp/news/2023/12/28/asia-pacific/politics/chinese-spy-agency-cia/.
47. Wong, et al., "Chinese Spy Agency Rising to Challenge the CIA."
48. Yang Sheng and Zhang Yuying, "Anti-Espionage Efforts of China Against U.S. Spies 'Essential, Effective,' " (December 27, 2023), China: *The Global Times*, https://www.globaltimes.cn/page/202312/1304440.shtml.
49. Benedict Vigers, "Confidence in U.S., UK Governments Lowest in G," (July 3, 2023). *Gallup*, https://news.gallup.com/opinion/gallup/507950/confidence-governments-lowest.aspx.
50. Laura Silver, Christine Huang, Laura Clancy, Nam Lam, Shannon Greenwood, John Carlo Mandapat, and Chris Baranovski, "Comparing Views of the U.S. and China in 24 Countries," (November 6, 2023). *Pew Research*, https://www.pewresearch.org/global/2023/11/06/comparing-views-of-the-us-and-china-in-24-countries/
51. Zen Soo, "China's Exports in November Edged Higher for the First Time in 7 Months, While Imports Fell," (December 7, 2023). *AP News*, https://apnews.com/article/china-exports-imports-decline-economy-7eabaf75c502f943afdd122e12b26dc.
52. Jana Puglierin and Pawel Zerka, "Keeping America Close, Russia Down, and China Far Away," (June 7, 2023). *European Council on Foreign Relations*, https://ecfr.eu/publication/keeping-america-close-russia-down-and-china-far-away-how-europeans-navigate-a-competitive-world/.
53. Ambassador Mark A. Green, "China is the Top Trading Partner to More Than 120 Countries," (January 17, 2023). *Wilson Center*, https://www.wilsoncenter.org/blog-post/china-top-trading-partner-more-120-countries; Igor Patrick, "China's Latin American Investments Downshift to Smaller, More Strategic Projects," (February 22, 2024). *SCMP News*, https://www.scmp.com/news/china/article/3252865/chinas-latin-american-investments-downshift-smaller-more-strategic-projects; Marcus Vinicius de Freitas, "The Impact of Chinese Investments in Africa: Neocolonialism or Cooperation?´(August 2023), *Policy Center for the New South (PCNS)*, Morocco, https://www.policycenter.ma/sites/default/files/2023-08/PB_30-23_Marcus%20Freitas.pdf; and Cissy Zhou, "Chinese Investment in Asia Rose 37% in 2023, Led by Indonesia," (March 7, 2024). *Nikkei Asia*, https://asia.nikkei.com/Spotlight/Belt-and-Road/Chinese-investment-in-Asia-rose-37-in-2023-led-by-Indonesia.

NOTES

54. Michael Shurkin, "Macon in Beijing: Why U.S.-China Watchers Need to Take a Deep Breath," (April 13, 2023). *The Hill*, https://thehill.com/opinion/international/3948006-macron-in-beijing-why-us-china-watchers-need-to-take-a-deep-breath/.
55. Jared Cohen, "The Global Credibility Gap," (December 6, 2023). *Foreign Policy*, https://foreignpolicy.com/2023/12/06/global-geopolitics-credibility-us-china-competition-alliances-deterrence-military-economic-power/.
56. *Congressional Research Service*, "U.S. Role in the World," (April 6, 2020), https://crsreports.congress.gov/product/pdf/R/R44891/47.
57. Myah Ward and Jonathan Lemire, "Biden: America at an Inflection Point in Israel and Ukraine," (October 19, 2023). *Politico*, https://www.politico.com/news/2023/10/19/biden-terrorist-must-pay-a-price-for-their-terror-00122644.
58. Edward Helmore, "Saudi Arabia and UAE Leaders 'Decline Calls With Biden' Amid Fears of Oil Price Spike," (March 8, 2022). *The Guardian*, https://www.theguardian.com/us-news/2022/mar/09/saudi-arabia-and-uae-leaders-decline-calls-with-biden-amid-fears-of-oil-price-spike; *Reuters,* "U.S. In Touch With Beijing About Arranging Military Communication," (December 12, 2023). https://www.reuters.com/world/us-touch-with-beijing-about-arranging-military-communication-pentagon-2023-12-12/; Sabrina Martin, "Iran Humiliates Joe Biden: Will Use Unfrozen Money As It Pleases," (September 13, 2023). *Vox*, https://voz.us/iran-humiliates-joe-biden-will-use-unfrozen-us-money-as-it-pleases/?lang=en.
59. Shane Tews, "China Challenges Multi-Stakeholder Model of Internet Governance," (December 23, 2015). *AEI*, https://www.aei.org/technology-and-innovation/china-challenges-multi-stakeholder-model-internet-governance/.