INSTITUTE FOR DEFENSE ANALYSES

The Cyber-Nuclear Nexus in a Geopolitical Condition of Competition

Michael P. Fischerkeller, Project Leader

August 2023

IDA Product 3000402

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under Project C5224, "Review and Editorial Prep for Non-sponsored Articles and Essays for External Publication," for the IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For More Information

Michael P. Fischerkeller, Project Leader
mfischer@ida.org, 703-845-6784

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Rigorous Analysis | Trusted Expertise | Service to the Nation

The Cyber-Nuclear Nexus in a Geopolitical Condition of Competition

Michael P. Fischerkeller

Most cyber scholars looking at the nexus of cyber campaigns/operations and the nuclear weapons enterprise—command and control, communications, and delivery systems/platforms—focus on scenarios of escalation between nuclear-armed states in militarized crisis or armed conflict.[1] Additionally, this scholarship focuses on the dependent variable of dyadic nuclear strategic stability. If we consider militarized crises and armed conflicts as geopolitical conditions, there is a third geopolitical condition—competition—where the nexus may generate consequences that, although of a different ilk, are no less consequential. Where the immediate consequence of targeting an opponent's nuclear weapons enterprise in militarized crisis and armed conflict could be *dyadic* nuclear strategic instability between the states involved, the immediate consequence of targeting the same in competition could be *global* geostrategic instability that would benefit no great power. This should further incentivize nuclear states to arrive at an explicit norm that makes the nuclear weapons enterprise a "no touch" zone for cyber campaigns/operations.

The Nuclear Umbrella

The crux of my argument rests on nuclear security guarantees. The United States provides extended strategic deterrence (a "nuclear umbrella") for around 30 non-nuclear allied states countries (many within the North Atlantic Treaty Organization), and also has notable arrangements of this type with South Korea, Japan, and Australia. Such guarantees are not limited to the United States. In December 2013, Ukrainian President Viktor Yanukovych and Chinese Communist Party leader Xi Jinping signed a bilateral treaty and published a joint statement where China reaffirmed a 1994 agreement in which it pledged "to provide Ukraine nuclear security guarantee when Ukraine encounters an invasion involving nuclear weapons or Ukraine is under threat of a nuclear invasion."[2] Additionally, as a key member of the Collective Security Treaty Organization, Russia ascribes to the language of Article 4 of the organization's

---

[1] For a discussion of what comprises the nuclear enterprise, see Herbert Lin, *Cyber Threats and Nuclear Weapons* (Stanford: Stanford University Press, 2021), https://www.sup.org/books/title/?id=34611 and Herbert Lin, "Cyber Risk Across the US Nuclear Enterprise," *Texas National Security Review* (Summer 2021): 107–120, http://dx.doi.org/10.26153/tsw/13986. To review scenario-based arguments, see Lin, *Cyber Threats and Nuclear Weapons*, chapter 5; Michael T. Klare, "Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation," *Arms Control Today*, November 2019, https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation; Jon Lindsay, "Cyber Operations and Nuclear Weapons", *NAPSNet Special Reports*, June 20, 2019, https://nautilus.org/napsnet/napsnet-special-reports/cyber-operations-and-nuclear-weapons/; Page O. Stoutland and Samantha Pitts-Kiefer, "Nuclear Weapons in the New Cyber Age: Report of the Cyber-Nuclear Weapons Study Group," *Nuclear Threat Initiative*, September 2018, https://media.nti.org/documents/Cyber_report_finalsmall.pdf; Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity* 3, no. 1 (March 2017): 37–48, https://doi.org/10.1093/cybsec/tyw017; and, Stephen J. Cimbala, "Nuclear deterrence and cyber: the quest for concept," *Air & Space Power Journal* (March 2014): 87–107, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-28_Issue-2/V-Cimbala.pdf.

[2] Gertz, Bill. "Putin's War Tests China's Nuclear Pact with Ukraine," *The Washington Times*, February 28, 2022, https://web.archive.org/web/20220302044101/https://www.washingtontimes.com/news/2022/feb/28/putins-war-tests-chinas-nuclear-pact-ukraine/.

treaty, which establishes that an aggression against one signatory would be perceived as an aggression against all.[3]

If it is revealed in a geopolitical condition of competition that the nuclear weapons enterprise of the U.S., China, and/or Russia has been compromised by cyber intrusions, no matter the source of those intrusions, the credibility of the nuclear security guarantees provided by the U.S., China, and/or Russia would be undermined—second strike would no longer be assured. The consequence of this on global geostrategic stability could be substantial.

States who formerly benefitted from nuclear security guarantees could, depending on their geostrategic circumstances, decide to pursue security through alternative ways and means, including significantly increasing their investments in conventional capabilities and force structure and pursuing nuclear weapons development programs. The former could lead to arms races that destabilize regional subsystems, and the latter would further complicate global nuclear dynamics as states abandon their commitments to the Nuclear Nonproliferation Treaty.

Are this revelation and these consequences plausible? The recent disclosure that North Korea compromised a Russian missile engineering company, and a "natural experiment" where the commitment of the nuclear umbrella was called into question suggests that they are.[4]

Disclosure

On August 7, 2023, SentinelLabs published a report noting that "[W]hile conducting our usual hunting and tracking of suspected-North Korean threat actors, we identified a leaked email collection containing an implant with characteristics related to previously reported DPRK-affiliated threat actor campaigns."[5] The target of North Korea's cyber campaign was NPO Mashinostroyeniya, a Russian company that is a pioneer developer of hypersonic missiles, satellite technologies and newer generation ballistic armaments.[6] The email archive included exchanges between NPO information technology (IT) staff highlighting questionable communications between specific processes and unknown external infrastructure. Security analysts at SentinelLabs identified the archive after discovering that an NPO IT staffer accidentally leaked his company's internal communications while attempting to investigate the

[3] https://treaties.un.org/doc/Publication/UNTS/Volume%201894/volume-1894-I-32307-Other.pdf.

[4] Natural experiments may be broadly understood as including an event not under the control of a researcher that divides a population into exposed and unexposed groups. See Peter Craig, Srinivasa Vittal Katikireddi, Alastair Leyland, and Frank Popham, "Natural Experiments: An Overview of Methods, Approaches, and Contributions to Public Health Intervention Research," *Annual Review of Public Health* 38 (March 2017): 39–56, https://doi.org/10.1146/annurev-publhealth-031816-044327.

[5] Tom Hegel and Aleksandar Milenkoski, "Comrades in Arms? North Korea Compromises Sanctioned Russian Missile Engineering Company," *SentinelLabs*, August 7, 2023, https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/.

[6] James Pearson and Christopher Bing, "Exclusive: North Korean Hackers Breached Top Russian Missile Maker," Reuters, August 7, 2023, https://www.reuters.com/technology/north-korean-hackers-breached-top-russian-missile-maker-2023-08-07/,

North Korean attack by uploading evidence to a private portal used by cybersecurity researchers worldwide.[7]

For the purposes of this essay, there are two important takeaways from the SentinelLabs report. First, they discovered the email tranche over the course of *routine business practices*. And second, the information was posted by a staffer of the Russian firm by *accident*. There is nothing exceptional about either of these circumstances. Regarding accidental postings, if one presumes that such information regarding similar U.S. technologies is classified, "classified spillage" is "incredibly common" according to former intelligence officials and attorneys who specialize in cases involving classified information.[8] One would expect the highest controls on nuclear enterprise-associated programs, which would lessen the likelihood of accidental spillage but likely not eliminate it.

Additionally, disclosures may be intentional actions by insiders motivated by various reasons. In 2016, a U.S. contractor shared the details of Russia's 2016 intrusions into U.S. election systems with the media, because they felt that the American people were "being led astray."[9] In addition, an anonymous person provided confidential documents from NTC Vulkan, a contractor working for Russia's military and intelligence establishment, to the German media, stating that "The company is doing bad things, and the Russian government is cowardly and wrong" and "I am angry about the invasion of Ukraine and the terrible things that are happening there … I hope you can use this information to show what is happening behind closed doors."[10] The cache of information included manuals, technical specification sheets, and other details for software designed by NTC Vulkan, as well as internal company emails, financial records, and contracts that show the ambition of Russia's cyber operations and the breadth of its outsourcing efforts.[11]

In sum, the disclosure of a compromise of a state's nuclear weapons enterprise is plausible.

A Natural Experiment

The success of extended strategic deterrence fundamentally rests on two factors: perceptions of the credibility of will and the credibility of capability. U.S. policy and actions in the previous administration cast unprecedented doubt on U.S. commitments to the nuclear security of its European and Australasian allies (i.e., credibility of will).[12] In June 2018, after the G-7 Summit, but before the NATO and Helsinki Summits, then-German Foreign Minister Heiko stated that "Part of the new transatlantic reality is that

---

[7] Ibid.

[8] Jeremy Herb, Katie Bo Lillis, Katelyn Polantz, and Zachary Cohen, "'I Had to Sleep with That Document': How the Government Tries to Prevent Classified Government Documents from Spilling Out," *CNN Politics*, January 24, 2023, https://www.cnn.com/2023/01/19/politics/classified-documents-spillage/index.html.

[9] "Reality Winner Says She Leaked Classified Material to Serve American People," *CBS News*, December 3, 2021, https://www.cbsnews.com/news/reality-winner-60-minutes-2021-12-03/.

[10] Craig Timberg, Ellen Nakashima, Hannes Munzinger, and Hakan Tanriverdi, "Secret Trove Offers Rare Look into Russian Cyberwar Ambitions," *The Washington Post*, March 30, 2023, https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/.

[11] Ibid.

[12] Susan J. Koch, "Extended Deterrence and the Future of the Nuclear Nonproliferation Treaty," Center for Global Security Research, August 2018, https://cgsr.llnl.gov/content/assets/docs/Security_Assurances_and_NPT_8-29.pdf.

we need to take on more responsibility for our own security because we can no longer count on the other side of the Atlantic doing so for us."[13] The same theme was echoed in July 2018 by then-Australian Prime Minister Tony Abbott, who stated "I fear there will have to be a much greater focus on strategic deterrence, especially if a rogue state like North Korea has long-range nuclear weapons—and especially if the American nuclear shield becomes less reliable."[14]

In this same political environment, Republican presidential front-runner Donald Trump's 2016 accusations that South Korea was free-riding has had an enduring and increasing impact on the views of the South Korean leadership and populace, with some of the former and most of the latter believing that America's security guarantees are only as good as its next leader. Opinion polls from 2017 revealed that about two-thirds of South Korean respondents said they supported their country once again hosting tactical nuclear weapons as it did prior to 1991.[15] More recently, three quarters of the populace has expressed support for South Korea to develop its own nuclear weapons.[16] In a 2017 interview Suh Kune-yull, a professor of nuclear engineering at Seoul National University, said, "If we decide to stand on our own feet and put our resources together, we can build nuclear weapons in six months."[17]

A recent agreement in which the U.S. committed to periodically deploying nuclear-armed submarines to South Korea and to involve Seoul in nuclear planning operations in exchange for a commitment by South Korea to not develop nuclear weapons has not placated those who want South Korea to develop its own arsenal.[18] In response to the agreement, Dr. Cheong Seong-chang said that, although the declaration had many positive aspects, it was "extremely regrettable that South Korea had openly given up its right to withdraw from the Nuclear Non-Proliferation Treaty," adding that this had "further strengthened our nuclear shackles."[19]

Finally, whereas Japanese public support for nuclear weapons historically remained low, it more than doubled (5% to 12%) from 2016 to 2017.[20] The increase in Japan may be attributed to statements made by then-U.S. Secretary of State Rex Tillerson during a visit to Japan in March 2017. When speaking to the nuclear threat posed by North Korea, Tillerson stated publicly that the United States might support

---

[13] Heiko Maas, "Germany's Foreign Minister Calls for 'A Real European Security and Defense Union,'" June 14, 2018, https://www.atlanticcouncil.org/blogs/natosource/germany-s-foreign-minister-calls-for-a-real-european-security-and-defense-union/.

[14] Tony Abbott, "An Ally Sizes Up Donald Trump," *The Wall Street Journal*, July 13, 2018, https://www.wsj.com/articles/an-ally-sizes-up-donald-trump-1531521949.

[15] Michelle Ye Hee Lee, "More Than Ever, South Koreans Want Their Own Nuclear Weapons," *The Washington Post*, September 13, 2017, https://www.washingtonpost.com/news/worldviews/wp/2017/09/13/most-south-koreans-dont-think-the-north-will-start-a-war-but-they-still-want-their-own-nuclear-weapons/.

[16] Jean Mackenzie, "Nuclear Weapons: Why South Koreans Want the Bomb," *BBC News*, April 22, 2023, https://www.bbc.com/news/world-asia-65333139.amp.

[17] Quoted in Carlos Ballesteros, "If North Korea Is Preparing for Nuclear War, All of Asia Needs Nuclear Weapons, Says Henry Kissinger," *Newsweek*, October 29, 2017, https://www.newsweek.com/north-korea-proliferation-nuclear-695787.

[18] Jean Mackenzie in Seoul & Barbara Plett Usher, "US and South Korea Agree Key Nuclear Weapons Deal," April 26, 2023, https://www.bbc.com/news/world-us-canada-65404805.amp.

[19] Ibid (quoted).

[20] Shibley Telhami, "Americans and Japanese Are Pessimistic About Ending North Korea's Nuclear Program and Oppose Military Options. Where Does That Leave Them?" January 22, 2018, https://www.brookings.edu/blog/order-from-chaos/2018/01/22/americans-and-japanese-are-pessimistic-about-ending-north-koreas-nuclear-program-and-oppose-military-options-where-does-that-leave-them/.

Japanese acquisition of nuclear weapons (for mutual deterrence reasons) if the North Korean threat is not resolved.[21] The only significant barrier preventing Japan from developing nuclear weapons is the security it obtains from relying on the United States.[22] Japan's nuclear latency ensures that a nuclear weapon is "a screwdriver's turn away."[23] In combination with missile technologies developed by the Japanese Aerospace Exploration Agency, Japan could rapidly develop its own strategic nuclear deterrent.

These reactions to a changed perception of the credibility of U.S. nuclear security guarantees suggest that similar dynamics would emerge if it was disclosed that a state's nuclear weapons enterprise had been compromised via a cyber campaign/operation. Even if the targeted state sought to reassure that it had the will to fulfill a commitment, the perception of an assured capability to carry out a nuclear threat could be undermined. It is reasonable to conclude that states who enjoy nuclear security guarantees from China and Russia would react similarly. Importantly, the U.S., China, and Russia would all be subject to the geostrategic instability that would likely result from such a perception, no matter for which state(s) that perception is held and no matter the agent behind the cyber campaign/operation that compromised the enterprise.

When Proliferation Optimists Become Pessimists

A scenario where a nuclear weapons enterprise is compromised through cyber ways/means might even turn proliferation optimists into pessimists. In 1990, John Mearsheimer considered alternative futures for Europe following the collapse of the Soviet Empire and proposed that the least dangerous scenario for maintaining peace in Europe was one in which nuclear weapons proliferate in Europe through a well-managed process overseen by the then-nuclear powers.[24] Importantly, however, Mearsheimer commented that "it is not likely that proliferation would be well-managed."[25] Moreover, he commented

---

[21] Jesse Johnson, "Amid North Korean Threat, Tillerson Hints That 'Circumstances Could Evolve' for a Japanese Nuclear Arsenal," *The Japan Times*, March 19, 2017, https://www.japantimes.co.jp/news/2017/03/19/national/amid-north-korea-threat-tillerson-hints-circumstances-evolve-japanese-nuclear-arsenal/. The Trump administration's remarks continue to influence Japanese senior leaders' views to this day. In November 2022, retired Admiral Kawano Katsutoshi, the longest-serving chief of Japan's Self-Defense Forces' Joint Staff under the Abe Shinzo administration, stated "Regarding the United States' nuclear umbrella, even if Washington says, 'you don't have to worry about it,' a suspicion crosses my mind. Is it really okay?" He specifically pointed out that former U.S. President Donald Trump used to profess Americans shouldn't sacrifice their lives to fight for other nations under his "America First" policy. Takahashe Kosuke, "Japan, South Korea Wonder: How Strong Is the US Nuclear Umbrella?" *The Diplomat*, January 7, 2023, https://thediplomat.com/2023/01/japan-south-korea-wonder-how-strong-is-the-us-nuclear-umbrella/.

[22] Dennis Lee, "A Nuclear Japan: The Push for Weaponization," *Harvard International Review*, August 18, 2019, https://hir.harvard.edu/a-nuclear-japan-the-push-for-weaponization/.

[23] Joseph F. Pilat, *Exploring Nuclear Latency: Report of a Workshop on Nuclear Latency Woodrow Wilson International Center for Scholars Washington D.C*," October 12, 2014, https://www.wilsoncenter.org/publication/exploring-nuclear-latency.

[24] John J. Mearsheimer, "Back to the Future: Instability in Europe after the Cold War," *International Security* 15, no. 1 (Summer 1990): 5–56, 8, https://www.jstor.org/stable/2538981.

[25] Ibid, 37.

that “proliferation is more likely to happen under disadvantageous international conditions than in a period of calm,” which in turn places an even greater burden on management.[26]

It is likely that the disclosure of a cyber-enabled disruption would be an unexpected and thus a “sudden” event, as are the disclosures of most significant cyber campaigns/operations. This, coupled with the reality that several states who currently enjoy security guarantees are nuclear latent states,[27] suggests that a revelation could result in unanticipated and rapid proliferation, thereby putting managed proliferation at risk. Additionally, the poor state of relations between the U.S. and China and the U.S and Russia, and the hostility between Europe and Russia and many Indo-Pacific countries and China, arguably represents “disadvantageous international conditions” and thus further strains managed proliferation.

Conclusion

For over a decade, states have been experimenting in and through cyberspace to identify novel cyber ways/means short of threats and uses of force to secure and/or advance their national interests in a geopolitical condition of competition. A successful compromise of another’s nuclear weapons enterprise in competition carries with it the risk of disclosure, which in turn could fuel global geostrategic instability, a significant consequence that has received little attention. States could, of course, seek to reassure allies about technical reliability much as they do with credibility of will. Alternatively, there ought to be reinvigorated efforts to develop an explicit nuclear power agreement to forego cyber campaigning in competition that targets nuclear weapons enterprises.[28] Credible nuclear possession is vitally important for the U.S., China, and Russia and thus the basis for formally negotiated parameters ought to be viable.

The views in this article do not necessarily reflect those of the U.S. Department of Defense or the U.S. Government.

[26] Ibid, 40.

[27] Mark Fitzpatrick, *Asia's Latent Nuclear Powers: Japan, South Korea and Taiwan* (International Institute for Strategic Studies, February 2016), https://www.iiss.org/publications/adelphi/2015/asia39s-latent-nuclear-powers-japan-south-korea-and-taiwan.

[28] President Biden reportedly raised this issue with President Putin at their June 2021 Geneva Summit. David E. Sanger, “Once Superpower Summits Were About Nukes. Now Its Cyberweapons,” *New York Times*, June 15, 2021, https://www.nytimes.com/2021/06/15/world/europe/biden-putin-cyberweapons.html.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-08-23	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Cyber-Nuclear Nexus in a Geopolitical Condition of Competition	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Michael P. Fischerkeller	C5224
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 730 East Glebe Road Alexandria, VA 22305	IDA Product 3000402

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Institute for Defense Analyses 730 East Glebe Road, Alexandria, VA 22305	IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A. Approved for public release: distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Michael P. Fischerkeller

14. ABSTRACT

Most cyber scholars looking at the nexus of cyber campaigns/operations and the nuclear weapons enterprise—command and control, communications, and delivery systems/platforms—focus on scenarios of escalation between nuclear-armed states in militarized crisis or armed conflict. Additionally, this scholarship focuses on the dependent variable of dyadic nuclear strategic stability. If we consider militarized crises and armed conflicts as geopolitical conditions, there is a third geopolitical condition—competition—where the nexus may generate consequences that, although of a different ilk, are no less consequential. Where the immediate consequence of targeting an opponent's nuclear weapons enterprise in militarized crisis and armed conflict could be *dyadic* nuclear strategic instability between the states involved, the immediate consequence of targeting the same in competition could be *global* geostrategic instability that would benefit no great power. This should further incentivize nuclear states to arrive at an explicit norm that makes the nuclear weapons enterprise a "no touch" zone for cyber campaigns/operations.

15. SUBJECT TERMS

Cyber strategy, cyber norms, nuclear enterprise

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Institute for Defense Analyses
Unclassified	Unclassified	Unclassified	Unlimited	6	19b. TELEPHONE NUMBER (Include Area Code)