Stanton Nuclear Security Fellows Seminar

PANEL 4: Nuclear Weapons in the US and Europe

1. Lauren Borja, CISAC

The Cyber Insider Threat to the U.S. Arsenal

According to the Director of the U.S. National Counterintelligence and Security Center, "All organizations are vulnerable to insider threats from employees who may use their access to facilities, personnel or information to harm their organizations—intentionally or unintentionally."[1] Insider attacks are defined as attacks on organizations carried out by either employees or affiliated personnel, such as independent contractors. While some insider attacks are accomplished through physical means,[2] cyberspace offers additional methods for execution. One example of a cyber insider attack is an employee that either knowingly or inadvertently gives hackers access to an organization's internal network. Furthermore, the cyber insider threat is dynamic, which requires organizations to frequently update their protective measures.[3]

In the U.S. nuclear arsenal, two incidents have demonstrated the danger posed by cyber insider attacks. In 1981, a nuclear missile officer attempted to give Russian diplomats the "cryptological procedures" used in the missiles along with "design capabilities and vulnerabilities of the Titan II weapons system..."[4] While no attack resulted from this disclosure, these procedures describe aspects of the computers that interface with U.S. nuclear missiles. Secondly, the Stuxnet worm, which targeted Iranian uranium centrifuges, spread using removable storage drives, such as USBs.[5] According to the Stuxnet dossier released by a cybersecurity firm that investigated the virus, "This may have occurred by infecting a

---

1 NCNS News, "NCSC and the National Insider Threat Task Force Launch National Insider Threat Awareness Month in September 2019" (Washington, D.C.: The National Counterintelligence and Security Center, September 3, 2019), https://www.dni.gov/index.php/ncsc-newsroom/item/2037-ncsc-and-the-national-insider-threat-task-force-launch-national-insider-threat-awareness-month-in-september-2019.

2 Matthew Bunn and Scott D. Sagan, eds., *Insider Threats*, 1 edition (Ithaca, NY: Cornell University Press, 2017).

3 Three editions of this cybersecurity guide have been released in the last seven years: Michael Theis et al., "Common Sense Guide to Mitigating Insider Threats, Sixth Edition" (Carnegie Mellon University: Software Engineering Institute, December 2018), https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644.

4 George Lardner, "Spy Rings of One," *Washington Post*, December 4, 1983, https://www.washingtonpost.com/archive/lifestyle/magazine/1983/12/04/spy-rings-of-one/aff2143a-7a19-4d8f-98b7-613c7bfebdf9/.

5 Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair*, March 2011, https://www.vanityfair.com/news/2011/03/stuxnet-201104.

willing or unknown third party, such as a contractor who perhaps had access to the facility, or an insider."[6]

Research question: What is the definition of a cyber insider attack to U.S. nuclear weapons? Because cyber insiders represent an evolving threat to the U.S. nuclear arsenal, further definition of the problem will enable policy makers to mitigate its effects. To classify this threat, I will consider four questions.

1. What is "inside" when talking about cyber insider attacks? In the physical world, established boundaries, like a building or fence, separate the inside from the outside; insiders cross these thresholds. Computers, however, are often part of vast networks and often interface with other external systems, blurring the line between inside and outside.[7] This lack of distinction between inside and outside also exists for all U.S. weapon systems, which are highly computerized: "weapon systems have a wide variety of interfaces, some of which are not obvious, that could be used as pathways for adversaries to access the systems..."[8] This blurring also exists within nuclear weapons systems. The computers used in nuclear weapon systems are built by military contractors with global supply chains. Furthermore, the officers in control of nuclear weapons are simultaneously connected to other military networks, such as those used for command and control.

2. What is the scope of potential damage caused by cyber insider attacks? Not all insider attacks lead to catastrophic failures. The following examples illustrate two different possibilities: a) In 2008, a virus infected both the unclassified and classified U.S. military networks. Because the virus was not specifically designed to target the network, some of its capabilities were not unleashed. Regardless, the Pentagon spent over a year eradicating the virus from its networks.[9] b) The Stuxnet virus infected Iranian centrifuges at the Natanz uranium enrichment facility multiple times between 2009-2010. These attacks delayed Iran's planned expansion of the facility, impacting its uranium enrichment capabilities.[10]

3. How can U.S. nuclear weapons be protected from both malicious and inadvertent cyber insider attacks? Insider attacks can be both malicious, where the insider is cognizant of the impact of their actions, and inadvertent, where the insider in unaware of the attack or their participation. While malicious attacks make up the bulk of physical insider attacks,[11] there is a growing awareness of the

---

6 Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier" (Symantec, February 2011), 3, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

7 Christian W. Probst et al., *Insider Threats in Cyber Security* (Springer Science & Business Media, 2010), https://www.springer.com/us/book/9781441971326.

8 GAO, "Weapon Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities" (Washington, D.C.: United States Government Accountability Office, October 2018), 13.

9 Ellen Nakashima, "Defense Official Discloses Cyberattack," August 25, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html.

10 David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz," Text (Washington, D.C.: Institute for Science and International Security, February 16, 2011), http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8.

11 Bunn and Sagan, *Insider Threats*.

threat due to inadvertent insiders in cyberspace.[12] Because they do not display the same warning signs, guarding against both types of insider could pose a challenge.

4. Do problems with cyber attack attribution further incentivize insiders? Attribution in many cyber attacks is challenging.[13] According to the 2017 U.S. State of Cybercrime report, which surveys organizations from commercial and government sectors, victims of cybercrime can often lack crucial information about an attack that would allow them to bring their attackers to justice.[14] As many of the cases listed herein show, insiders are rarely identified publicly after an attack. How do insiders view the anonymity offered by cyberspace?

To answer these questions, I will investigate recommendations from the cybersecurity field for preventing the insider threat and current cyber security and cyber hygiene practices in the U.S. nuclear arsenal. There is extensive literature from the computer security field on insider threats. To address current practices in the U.S. nuclear arsenal, I will look at safety procedures for nuclear weapons and reports from various government agencies on nuclear weapon systems.[15]

Clarifying the cyber insider threat to U.S. nuclear weapons will help develop policy towards its mitigation. My proposed research fits into ongoing work on the nuclear security,[16] previous studies on the insider threat to nuclear facilities and material management,[17] and cybersecurity of U.S. nuclear

12 Recent updates to the CMU/SEI manual on insider threats have added emphasis on the danger of inadvertent data loss, see Theis et al., "Common Sense Guide to Mitigating Insider Threats, Sixth Edition," 2.

13 Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," *Columbia Journal of International Affairs, Forthcoming*, 2016, Available at SSRN: https://ssrn.com/abstract=2835719.

14 Sarah Miller, "2017 U.S. State of Cybercrime Highlights," *Carnegie Mellon University Software Engineering Institute* (blog), January 17, 2018, https://insights.sei.cmu.edu/insider-threat/2018/01/2017-us-state-of-cybercrime-highlights.html.

15 The Federation of American Scientists maintains a database of U.S. Air Force technical documents; see Steven Aftergood, "Air Force Intelligence and Security Doctrine," September 9, 2019, https://fas.org/irp/doddir/usaf/index.html; for information from other government agencies, see Thomas P. Christie, "Minuteman III Guidance and Propulsion Replacement Programs," Annual Report, FY2002 Annual Report (The Office of the Director, Operational Test and Evaluation (DOT&E), January 2003), http://www.dote.osd.mil/pub/reports/FY2002/pdf/af/2002MinutemanIIIGPRP.pdf; Cristina T. Chaplain, "Nuclear Command, Control, and Communications: Update on DOD's Modernization" (Washington, D.C.: Government Accountability Office, June 15, 2015), https://www.gao.gov/products/GAO-15-584R; Theresa Hull, "Air Force Space Command Supply Chain Risk Management of Strategic Capabilities" (Washington, D.C.: Department of Defense, Office of the Inspector General, August 14, 2018), https://media.defense.gov/2018/Aug/16/2001955109/-1/-1/1/DODIG-2018-143_REDACTED.PDF.

16 Matthew Bunn, Nickolas Roth, and William H. Tobey, "Revitalizing Nuclear Security in an Era of Uncertainty" (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, January 2019), https://www.belfercenter.org/sites/default/files/2019-03/RevitalizingNuclearSecurity_Mar19.pdf.

17 Bruce Hoffman et al., "Insider Crime: The Threat to Nuclear Facilities and Programs," Product Page (Santa Monica, CA: RAND, 1990), https://www.rand.org/pubs/reports/R3782.html; International Atomic Energy Agency, "Preventive and Protective Measures against Insider Threats," Text, Nuclear Security Series (Vienna: IAEA, September 6, 2016), https://www.iaea.org/publications/7969/preventive-and-protective-measures-against-insider-threats; Andrew N Healey, "The Insider Threat to Nuclear Safety and Security," *Security Journal* 29, no. 1 (February 1, 2016): 23–38, https://doi.org/10.1057/sj.2015.42; Bunn and Sagan, *Insider Threats*.

forces.[18] While some previous discussions included both cyber and physical insider attacks,[19] my focus on the insider threat in cyberspace will allow me to bring further attention to certain aspects that are more relevant in this space, such as inadvertent insiders and the lack of attribution in cyberattacks. This work is an application of research on the cyber insider threat in the field of computer science.[20] While relevant for defining and clarifying the scope of the cyber insider threat, these sources did not consider its impact on nuclear weapons.

Furthermore, this is relevant because of the current modernization plans to the U.S. nuclear arsenal and global rise in offensive cyber operations. According to the Congressional Budget Office, the United States plans to spend $494 billion over the next decade on refurbishing or replacing its nuclear weapons systems.[21] Decisions made during these extensive upgrades could impact cybersecurity of nuclear weapon systems for generations.[22] Furthermore, nation-states are vastly increasing their offensive cyber operations.[23] Many of the most sophisticated actors in this space are either possess or aspire to possess nuclear weapons, which could have potential implications for nuclear weapons security.

Challenges

It will be challenging to find documents describing current cybersecurity or cyber hygiene practices in the U.S. nuclear arsenal. Some information can be found for computer and software practices in the U.S. ICBM force;[24] information on nuclear bombers or nuclear ballistic missile submarines has been harder to find. Other suggestions for source material on cybersecurity practices in the U.S. nuclear arsenal are appreciated.

---

18 Jason Fritz, "Hacking Nuclear Command and Control" (May 2009), http://www.icnnd.org/Documents/Jason_Fritz_Hacking_NC2.pdf; Andrew Futter, "Hacking the Bomb: Cyber Threats and Nuclear Weapons" (Washington D.C.: Georgetown University Press, 2018), 208, http://press.georgetown.edu/book/georgetown/hacking-bomb; Lauren J. Borja, "Assessing Priorities towards Achieving Dependable and Secure Computing in the U.S. ICBM Force," *Science & Global Security*, accepted.

19 Healey, "The Insider Threat to Nuclear Safety and Security."

20 Probst et al., *Insider Threats in Cyber Security*; William F. Gross, "Insider Threat," in *Computer and Information Security Handbook*, 3rd ed. (Moran Kaufmann, 2017), 529–36, https://www.amazon.com/Computer-Information-Security-Handbook-Vacca/dp/0128038438; Theis et al., "Common Sense Guide to Mitigating Insider Threats, Sixth Edition."

21 Keith Hall, "Projected Costs of U.S. Nuclear Forces, 2019 to 2028" (Washington, D.C.: Congressional Budget Office, January 2019), https://www.cbo.gov/system/files/2019-01/54914-NuclearForces.pdf.

22 Peter H. Feiler et al., "Reliability Validation and Improvement Framework" (Pittsburgh, PA: Software Engineering Institute, Carnegie-Mellon University, November 2012), https://apps.dtic.mil/docs/citations/ADA610905.

23 Herbert Lin and Amy Zegart, eds., *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington, D.C: Brookings Institution Press, 2019).

24 Commander of the Air Force Global Strike Command, "Intercontinental Ballistic Missile (ICBM) Software Procedures," Nuclear, Space, Missile, Command and Control (Air Force, March 26, 2013), http://static.e-publishing.af.mil/production/1/afgsc/publication/afgsci13-5306/afgsci13-5306.pdf.

2. Andrea Chiampan, MIT SSP

Flawed Architects, Resilient Technologies, and the Making of the Second Cold War

INTRO

Flawed Architects, Resilient Technologies explores the origins of the "Euromissile Crisis" in the 1970s and early 1980s and sheds new light on the techno-political origins of the so-called "Second Cold War" – the renewed tension in international relations that characterized the late phase of the Cold War. Today, cruise missiles have unexpectedly returned to the center of the international security debate. The United States launched a modernization program of its nuclear cruise missile arsenal, while the Russian cruise missile threat has increased exponentially. Against this background, *Flawed Architects, Resilient Technologies* offers a fresh reflection on how technologies have shaped and continue to shape NATO's nuclear strategies.

BIG & SMALL QUESTIONS

The main questions that the research seeks to answer are two – one purely historiographical, the other more theoretical. *First*, why did NATO – in face of rising protest and unrest – decide to deploy additional 572 nuclear warheads in Europe mounted on intermediate-range missiles after it had relinquished such possession in the early 1960s and in total contradiction to half a decade of parliamentary and congressional pressure to reduce the number of nuclear weapons in Europe? *Secondly* – and this is the "big question" if you will – how do politics and technology interact and how does this interaction influence, determine, and ultimately construct US nuclear strategy? In other words, is there a logical, recognizable, and most importantly "efficient" relationship between nuclear strategy and the artifacts built and employed to achieve them? Understanding the *modus operandi* of this relationship may help us – and most importantly policymakers – not to accept passively existing strategic paths and not to ascribe to technological artifacts an unrestrainable agency they do not possess. More modestly, if anything, this research will shed new light and provide deeper understanding of both the origins of the "second Cold War" and the origins of today's bias towards "counterforce" missions that characterize the US military's and by extension NATO's nuclear posture.

METHODS & THEORY

The methodology to answer these questions is almost entirely historiographical. Through a detailed analysis of recently declassified primary documents held in a dozen of archives in key NATO countries – including the United States, Italy, Belgium, Germany, and the United Kingdom – *Flawed Architects, Resilient Technologies* dovetails the decision-making process within the US and NATO bureaucracies that led to the development and deployment of the cruise missile. This research also delves into how this decision-making process intertwined with the related debate about NATO's nuclear posture in Europe. This multi-archival and multi-lingual analysis is aided by theoretical frameworks and concepts adopted from SHOT (Social Construction of Technology) theory that provide important interpretative lenses and lexicon to give a broader outlook to the detailed analysis of the data obtained from the archives.

NARRATIVE & ARGUMENTS

Flawed Architects, Resilient Technologies is structured around two parallel developments taking place in the age of détente. On the one hand, the development of a weapon technology – the

cruise missile; on the other hand, the forging of arms control as a fundamental component of US grand strategy by its main architect – Henry Kissinger.

As it stands, the research shows how an array of "flawed architects" and "heterogenous engineers" took pivotal decisions regarding technological research, development, procurement that ultimately shaped not only US nuclear strategy but also transatlantic and superpowers' relations in the 1970s and 1980s. These decisions, however, were almost entirely disjointed both from technical and military-strategic considerations. Contrary to those views that one may broadly label as "technological determinism," which maintain that the revival of cruise missile technology was the result of the technological improvements in digital computers and inertial navigation systems of the late 1960s, and contrary to the expectation and assumption that cruise missiles responded to a military-strategic need, *Flawed Architects, Resilient Technologies* argues that the NATO's decision to procure the weapon was, in fact, largely the result of political miscalculations and compromises.

Arms control strategies, bureaucratic struggles erected by embattled neoconservative Congressmen, and transatlantic alliance management considerations shaped the controversial decision to endow NATO with these new weapons. Furthermore, *Flawed Architects, Resilient Technologies* unveils how unexpected and accidental transatlantic encounters and the unintended consequences of national political agendas came to shape NATO's decision. On the one hand, the agenda of key figures within the rising neoconservative bloc – in their attempt to sabotage the SALT negotiations – coalesced with those officials in the British government, who had come to fear the direction the SALT II negotiations were taking. For them, cruise missiles became an instrument to squander arms control and détente. On the other hand, many officials including Henry Kissinger and Chancellor Helmut Schmidt became convinced that cruise missiles should become the building block of the next round of SALT negotiations. All these elements conjured up leading NATO to deploy new weapons that the relevant military services in the U.S., Britain, and NATO had initially deemed militarily and strategically unnecessary. These convergencies and not the 1979 dual-track decision, in my view, marked the beginning of the Euromissile Crisis.

CONCLUSIONS

This episode shows how military technological innovation, far from being a natural evolution of scientific knowledge, is strongly shaped by political rather than military and technical constructs, which bolster or hinder certain patterns of development over others for reasons quite unrelated to scientific, technical and military motives. Furthermore, *Flawed Architects, Resilient Technologies* will point out how a seemingly unimportant routine R&D decision carried grave unintended consequences in spurring the onset of a "second Cold War." Finally, this research shows how the decisions of these flawed architects and heterogenous engineers resulted in the construction of "resilient technologies" – such as the cruise missile – that were instrumental in dragging the US military and its NATO allies towards the counterforce bias – a doctrine that continues to dominate US nuclear posture today.

THE EXISTING LITERATURE

The existing literature suffers from three main shortcomings. The *first* is "technological determinism." According to this view, technical developments, such as improvements in digital

computers, miniaturization of nuclear warheads, as well as a new inertial navigation aid known as TERCOM (Terrain Contours Recognition Matching) that made the modern cruise missile possible tantalized the military services' commands – always on the look for new gadgets – and finally reached the NATO machinery fascinated by the technical, military, and strategic virtues of the weapons. The *second* shortcoming we could call "technological under-determinism," which is a form of technological determinism of its own. Instances of technological under-determinism are ubiquitous in the literature on the origins of the Euromissile Crisis. Nearly all accounts acknowledge, for instance, that the resurgence of the cruise missile technology should be accounted amongst the causes for their eventual deployment, but these statements remain nothing more than condiment in the dual-track decision recipe. Ironically, by accepting the role of new technologies without clearly determining their contours, the risk is to give technical innovations an agency they do not possess. Both of these views tend to magnify the role of the "military-industrial-complex." A *third* shortcoming comes from an excessive reliance on the "rational military-strategy" explanation. According to this view, the decision to develop and deploy these weapons was to be ascribed to an existing military-strategic need to fill a gap in the spectrum of extended deterrence. This was the explanation NATO provided at the time. In the words of one US official involved in the NATO deployment negotiations, these new intermediate range missiles represented quite simply the "ultimate evolution" of NATO's nuclear posture. In addition, a version of this narrative portrays the decision as a logical military-and-politically-oriented response to Soviet re-armament of the mid-late 1970s.

RESEARCH CONTRIBUTION

In contrast to these views, *Flawed Architects, Resilient Technologies* argues that the story we should tell is one where technical "facts" all but disappear and leave space to constructed contingencies that have to do much more with the personalities of the people involved, with the economic realities that the Department of Defense had to face in the post-Vietnam era, with Henry Kissinger and his idea of détente, with the rise of SALT and its opposition – that is to say with the rise of neoconservatism – and with James Schlesinger's warfighting-and-counterforce-flavored strategic ideas and their contradictory implementation. As outlined above, the story this research tells is one of a "seamless web" of interactions between "heterogenous engineers," whose often contradictory and improvised decisions about research, development, and procurement constructed and paved the cruise missile path from the "black box" all the way to international intra-Alliance and inter-blocs crisis. *Flawed Architects, Resilient Technologies* suggests that by focusing on these interactions not only do the "military-industrial-complex," "technological determinism," or the "action-reaction" explanations become insufficient, but also the direct line that connects military strategy and the technologies that accompany them that has dominated the "Wizards of Armageddon" inspired literature becomes weaker. The main strength of *Flawed Architects, Resilient Technologies* is that, unlike existing accounts, it manages to recognize the strength, resilience, and ultimately the importance of technology, while at the same time recognizing the messy, contingent, and "un-technical" characteristics of the politico-socio-technical web of actors and networks within which technology is shaped.

POLICY CONTRIBUTION

The first policy contribution comes in the form of a warning by historical analogy. This research warns policymakers against the risk of letting technological innovation dictate grand strategy – as if technology stood in the international arena as an independent variable. Existing technical realities should not necessarily be taken as immutable on account of their presumed rational development, procurement, and employment. For instance, the idea often flaunted by US Air

Force officials that cruise missiles had been adopted to solve a military problem – the penetration of bombers against Soviet air defenses – proved to be historically incorrect. The fact that the US military continue to use this line of reasoning to argue for a new and improved generation of air-launched nuclear-armed cruise missile should be taken with great skepticism. Overall, the lesson to be learned from this case-study is that policymakers should always question whether weapon procurements correspond necessarily to military-strategic needs, as this was clearly not the case for the cruise missile.

Secondly, this research offers insight on how ill-advised weapon procurement decisions can trigger unintended consequences that hinder foreign policy. The decision to develop cruise missiles created an arms control problem that in the 1980s generated new international tensions and brought NATO to a near standstill. In recent years, the cruise missile problem has become a proliferation problem as well, with medium and small powers joining the cruise missile club (i.e. India, Pakistan, Iran, possibly North Korea), and with Russia redesigning its nuclear arsenal to give cruise missiles a more central role. To this regard, a second concrete policy recommendation stemming from this research comes in the form of an exhortation. The United States should take the lead in tackling the cruise missile proliferation problem – a problem it contributed to create – through a comprehensive and global arms control strategy. This should start with data exchange and confidence building measures to dilute the main obstacle against limitations on nuclear-armed cruise missiles: verification. The case-study analyzed in *Flawed Architects, Resilient Technologies* should persuade every policymaker of the centrality of comprehensive arms control regimes and procedures in any far-sighted grand strategy.

WEAKNESS

As a Stanton Fellow, I aim to improve the portion of my research that extends the historiographical narrative to contemporary politics and policy as this remains, in my view, the weaker and most vulnerable aspect of this study. The mentors' feedback on how to best complete this transition from historiographical to policy relevance would be most helpful.

3. Luke Griffith, RAND

The Quest for Stability in a Post-INF World: Learning from Jimmy Carter and Ronald Reagan

U.S. President Donald Trump and Russian President Vladimir Putin have threatened to launch a terrifying nuclear arms race. On August 2, 2019, Trump allowed the world's first nuclear disarmament agreement, the Intermediate-Range Nuclear Forces (INF) Treaty, which prohibited U.S. and Russian ground-based missiles capable of flying 500 to 5,500 kilometers, to lapse. On one hand, U.S. officials protested the Russian deployment of 9M729 intermediate-range cruise missiles. Lamenting the exclusion of thousands of Chinese weapons from the INF Treaty, Trump also labeled the accord a relic of the bipolar Cold War. On the other hand, Russian diplomats insisted the United States violated the agreement by stationing Mk-41 missile launchers in Europe as part of the Aegis Ashore theater missile defense system. Sixteen days after the INF Treaty expired, the Pentagon tested its first intermediate-range missile since the Cold War, and Putin pledged to showcase comparable systems. First-strike weapons, intermediate-range ballistic missiles destabilize the international system: they can destroy retaliatory forces and decapitate leadership in a matter of minutes, reducing deliberation time in a crisis. Today, Russia and the People's Republic of China are developing hypersonic, intermediate-range missiles capable of penetrating American defenses and wrecking targets on land and sea. The United States, American General John E. Hyten testified to the Senate Armed Services Committee in March 2018, lacks "any defense that could deny the employment of such a weapon against us."[25] If American missiles are deployed in Europe or Asia, retired Russian General Vladimir Bogatyryov speculated, Moscow might station systems in Venezuela or Cuba.[26]

In the coming years, U.S. officials are confronted with and potentially even preparing for the daunting prospect of a new arms race. "We'll have to develop those [INF] weapons," Trump explained on October 20, 2018, "unless Russia comes to us and China comes to us and they all come to us and say, 'Let's really get smart, and let's none of us develop those weapons.'"[27] More complicated, the United States lacks negotiating leverage: it has no comparable systems to exchange for 9M729s and Chinese intermediate-range missiles and, even if it develops a new generation of weapons, has limited basing options abroad.[28] Today, North Atlantic Treaty Organization (NATO) and Asian allies are cold to U.S. missile deployments, limiting basing locations to American territories, such as Guam. While it is prudent to seek constraints on Chinese systems, which cover targets throughout the First and Second Island Chains in the Pacific Ocean, U.S. policymakers have yet to outline a strategy to achieve that goal.

---

[25]R. Jeffrey Smith, "Hypersonic Missiles are Unstoppable. And They're Starting a New Global Arms Race," *The New York Times Magazine*, June 19, 2019.
[26]Vladimir Isachenkov, "Putin Orders Russia to respond after US Missile Test," *Associated Press,* August 23, 2019.
[27]"Remarks by President Trump Before Air Force One Departure," October 20, 2018, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-air-force-one-departure-4/ (accessed August 1, 2019).
[28]On INF hardware, see: Jacob Cohn, Timothy Walden, Adam Lemon, and Toshi Yoshihara, "Leveling the Playing Field: Reintroducing U.S. Theater-Range Missiles in a Post-INF World," Center for Strategic and Budgetary Assessments, Washington, D.C., 2019.

Relying on archival-based research and traditional historical methods, I will elucidate lessons from the late Cold War for American policymakers facing the aftermath of the INF Treaty's demise. By studying the 1970s and 1980s, the Trump administration or, depending on the outcome of the 2020 election, a Democratic successor might be able to avoid a reckless arms race that imperils world peace, strains relations with allies, and exacerbates tensions with Russia and China. To provide policy prescriptions, I will employ qualitative analysis derived from two case studies, examining the evolution of U.S. nuclear policy under President Jimmy Carter and President Ronald Reagan, the American leaders who secured the INF Treaty. I will also highlight commonalities between the late Cold War and 2019, explaining ways in which the present situation is unique. I will lean on primary research conducted at repositories in the United States and abroad, as well as digitized source collections, to analyze declassified government documents, such as memorandums and records of conversation from allied consultations, National Security Council meetings, and the NATO bodies designed to craft nuclear policy. Facing classification restrictions on current government documents, I will utilize public sources, such as newspaper articles, think tank studies, and press statements, to shed light on the present. I aim to answer several queries: how should American officials manage the death of the INF Treaty? What can they learn from Carter and Reagan? What proposals might prove effective during multilateral negotiations with Moscow and Beijing? Should they consider deploying a new generation of intermediate-range missiles? And how can they marshal allied and congressional support for U.S. nuclear policies?

If contemporary policymakers aspire to overcome allied basing reluctance and acquire bargaining chips, they should study the adroit transatlantic diplomacy of Carter, who rallied NATO support for a polarizing multilateral initiative, the dual-track decision, and allowed Reagan to approach the INF negotiations from a position of strength. Responding to a relentless buildup of Soviet SS-20 intermediate-range missiles in December 1979, Carter and NATO allies announced the dual-track decision, which called for the deployment of 572 U.S. missiles in Europe and simultaneous arms talks with Moscow. Previous scholars have painted West German Chancellor Helmut Schmidt as the architect of the two-track program, portraying Carter as an ineffective, bumbling leader of the Atlantic alliance. However, recent evidence reveals that Carter shaped the hardware package, the arms control approach, and the precise relationship between the two tracks in a fundamental way. Mindful of waxing anti-nuclear sentiments in Europe, Carter cooperated with NATO allies to craft a program that minimized domestic criticism of their governments. Eyeing skeptical European allies, Carter expanded the permanent membership of the Nuclear Planning Group, NATO's senior body on nuclear matters, and allowed European officials to dictate how ground-based missiles would be stationed on their soil. Carter also ensured the buildup would not increase the number of nuclear weapons in Europe, where he removed 1,000 aging American warheads. Equally important, Carter's dual-track approach reflected a realistic understanding of arms control: to persuade the Kremlin to dismantle hundreds of operational systems in Europe, where the United States lacked comparable weapons, Carter needed bargaining chips that provided a powerful incentive for Soviet officials to engage in productive negotiations.

Like today, the intermediate-range debate appeared intractable in the 1980s, when Reagan's patience, optimism, and commitment to arms reductions facilitated the INF Treaty. Ignorant of the arcane substance of arms control, Reagan was a tool for his skillful aides, previous scholars write. Reagan's zero

option proposal, requiring the liquidation of U.S. and Soviet intermediate-range missiles, was a hollow gesture designed to stalemate the negotiations and buy time for the United States to build up military strength. Reagan never devised the precise American proposals presented in Geneva, but he provided rigid guidelines for acceptable overtures that conformed to his arms control philosophy. Reagan wanted to negotiate from a position of strength, which required deployment of American missiles in Europe. However, Reagan was also a nuclear abolitionist: he recognized that modernization was a means to an end—arms reductions—and hounded the Kremlin for six years to verify the elimination of intermediate-range missiles. "We are not dealing with philanthropists," President Richard Nixon often reminded Reagan. "The Soviets…are not giving us SS-20s for nothing."[29] Frustrated by Soviet intransigence before General Secretary Mikhail Gorbachev, an amenable negotiating partner, assumed power in March 1985, Reagan remained patient with the stalemate, refusing to allow international crises, such as the downing of Korean Air Lines flight 007 in September 1983, to derail arms talks. Even more significant, Reagan and Gorbachev cultivated the atmosphere of trust required to authorize hundreds of on-site inspections, leading to the liquidation of 2,692 missiles and the elimination of an entire class of weapons.

There are also key dissimilarities between the late Cold War and 2019, however. First, the British, West Germans, and Italians were enthusiastic about nuclear modernization in the late 1970s. Today, American allies in Europe and Asia have yet to express willingness to host ground-launched systems. If the Russian and Chinese buildups continue unabated, though, U.S. allies might warm to a basing program when presented with a concrete American deployment plan and arms control strategy. Second, the Kremlin has not yet deployed large numbers of 9M729s in Eurasia, where Moscow stationed dozens of SS-20s by December 1979, when NATO announced counter deployments. Third, U.S. policymakers will not be negotiating with Gorbachev, who authorized the unilateral concessions that broke the INF deadlock, and should anticipate prolonged arms talks. Putin, in contrast, exerted minimal effort to preserve the INF Treaty. Finally, the presence of thousands of Chinese intermediate-range missiles will complicate U.S. efforts to forge a new INF accord. Xi, too, opposes the American notion of transforming the INF Treaty into a multilateral agreement. At the moment, Beijing has little to gain from negotiating with Moscow and Washington: there is no arsenal of intermediate-range weapons aimed at China, and U.S. and Russian officials have not offered significant concessions in return for constraints on Chinese systems. The INF Treaty was signed eight years after the dual-track decision was announced and, given the inferior American position today and added complexity of multilateral talks, negotiating a new deal will be even more arduous.

Guided by two case studies, I will explore policy options for American officials, who should formulate a dual-track strategy. Unlike the mid-1980s, when Reagan possessed hundreds of missiles to trade for SS-20s and negotiated with Gorbachev, who shared his dream of abolishing nuclear weapons, American arms controllers lack leverage vis-à-vis Russia and China, where there is little prospect of leadership change. Rather than proposing a new zero option, a gambit that will likely be rejected and impede progress in bilateral or multilateral arms talks, U.S. policymakers should pursue a more obtainable objective, such as a global ceiling on ground-launched, intermediate-range nuclear and conventional

[29]Memorandum for the Record, "Meeting with President Nixon," May 14, 1987, folder Ed Rowny 05/18/1987, box 4, Howard Baker Files, Ronald Reagan Library, Simi Valley, California.

missiles. A worldwide ceiling would control the Russian and Chinese buildups, preserving the American prerogative to station missiles abroad, which Washington does not need to exercise if negotiations prove productive. The threat of American deployments may force the Russians and Chinese to the negotiating table. A fruitful first step, a global ceiling would also pave the way for future disarmament talks, when American officials might suggest the abolition of all intermediate-range missiles. Equally important, they should consider coupling arms control overtures with conventional missile deployments, which would offset Russia and Chinese systems on the battlefield and negotiating table and prove less provocative than nuclear weapons. Regardless of the American approach, they must rally allied and congressional support for U.S. policies, cooperating to craft a strategy that allied political leaders will endorse. Like their predecessors in the 1980s, contemporary analysts doubt INF negotiations will be productive. Hopefully they are wrong again. "To some the zero option was impossibly visionary and unrealistic; to others merely a propaganda ploy," Reagan remarked on December 8, 1987. "Well, with patience, determination, and commitment, we've made this impossible vision a reality."[30]

[30]"Remarks on Signing the Intermediate-Range Nuclear Forces Treaty," December 8, 1987, https://www.reaganlibrary.gov/research/speeches/120887c (accessed August 1, 2019).