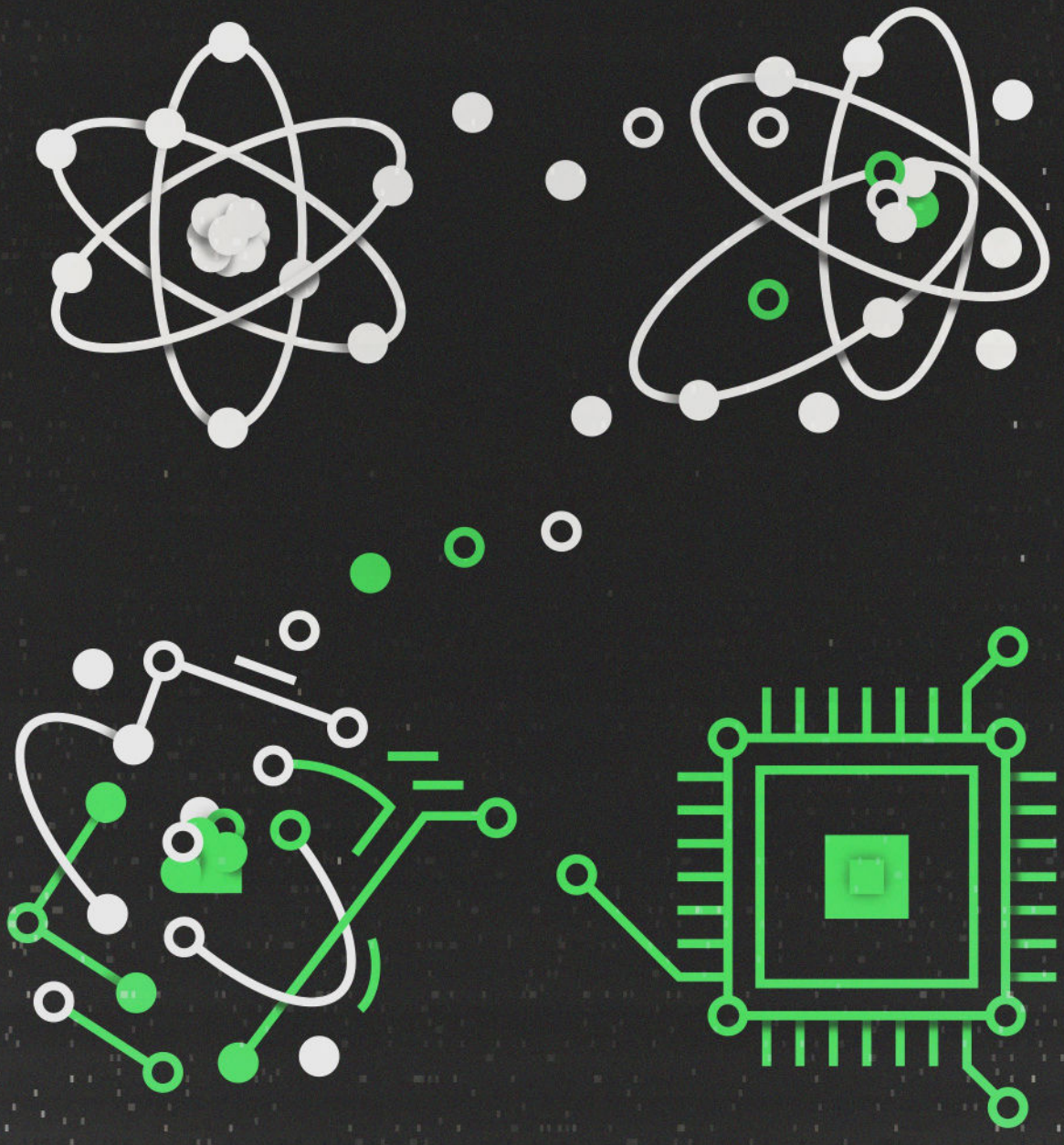
FOUNDATION FOR DEFENSE OF DEMOCRACIES

Lessons for the Cyber Battlefield from the Early Nuclear Era's Single Integrated Operating Plan

Brian M. Mazanec
January 2019

Foreword by
Samantha F. Ravich



Lessons for the Cyber Battlefield from the Early Nuclear Era's Single Integrated Operating Plan

Brian M. Mazanec

Foreword by
Samantha F. Ravich

January 2019

FDD PRESS

A division of the
FOUNDATION FOR DEFENSE OF DEMOCRACIES
Washington, DC

Table of Contents

FOREWORD 6

INTRODUCTION 8

RELEVANT HISTORICAL FACTORS PRECIPITATING THE NEED FOR A CYBER SIOP-LIKE PROCESS 10

PLANNING PROCESS LESSONS 12

- Integrating Participants through Framing Questions and Organizational Structures 12
- Using a Sequential and Interdependent Process with Capability Cutoff 16
- Increasing Information Needed to Drive Planning 17

TARGETING LESSONS 18

- Integrating Targeting and Developing Consistent Target Categories and Approaches 18
- Growing Intelligence Needed to Support Targeting 20
- Moving Toward Targeting Flexibility and Options 20

FORCE STRUCTURE/CAPABILITY REQUIREMENTS LESSONS 22

- Developing Indirect Relationship between Nuclear Planning and Force Structure/Capability Requirements 22
- Ensuring Planning Was Consistent with Existing and Available Force Structure 23

ALLIED ENGAGEMENT LESSONS 23

- Growing Allied Role in SIOP Development 23

CONCLUSIONS AND RECOMMENDATIONS 24

APPENDIX I: BACKGROUND ON EARLY NUCLEAR SIOPS 26

APPENDIX II: OVERVIEW OF DETERRENCE THEORY AND CYBER WARFARE 31

Foreword

By Samantha F. Ravich, Ph.D.

Dr. Ravich is the chairman of FDD's Center on Cyber and Technology Innovation and the principal investigator of its project on cyber-enabled economic warfare. She is the vice chair of the President's Intelligence Advisory Board and a member of the congressionally-mandated Cyberspace Solarium Commission.

When the Foundation for Defense of Democracies launched its Cyber-Enabled Economic Warfare project in 2016, U.S. cyber strategy was built on the Pentagon's April 2015 cyber strategy[1] and the White House's 2016 "Report on Securing and Growing the Digital Economy."[2] Both documents recognized that cyber attacks and cyber espionage had gained as much relevance to U.S. national security as conventional military activities and spycraft. However, they also revealed a gap in U.S. strategic thinking about how adversaries were exploiting developments in information technology to cause economic damage to America and its allies. These developments are prompting alarm over *cyber-enabled economic warfare*, a new form of economic warfare not well understood by decision-makers. And while the United States has increasingly relied on financial sanctions to influence international affairs, there is a paucity of analysis on how this new form of economic warfare could be deployed against the U.S. by its adversaries.

The Trump administration has begun to rectify this problem. Recognizing that cyberspace offers "state and non-state actors the ability to wage campaigns against American political, economic, and security interests without ever physically crossing our borders,"[3] the administration's December 2017 National Security Strategy explicitly warned that adversarial nations are "weakening our businesses and our economy as facets of cyber-enabled economic warfare and other malicious activities."[4] By their very nature, these operations are an attack against America's citizenry and not merely its military or government. Their ultimate goal is to undermine the engine of the country's strength – its economy – and compel or coerce the government to alter its behavior.

The subsequent National Cyber Strategy of 2018 warned that U.S. adversaries "view cyberspace as an arena where the United States' overwhelming military, economic, and political power could be neutralized and where the United States and its allies and partners are vulnerable."[5] The Pentagon's new Defense Cyber Strategy acknowledges that the Defense Department "must be prepared to defend non-DoD-owned Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) networks and systems," because civilian assets enable the U.S. military advantage.[6] Together, these strategy documents acknowledge that the United States is vulnerable and must position itself to defend critical economic capabilities.

Today's battlefield is unique because the U.S. government is joined on the front lines by the private sector. In the Cold War, citizens and businesses were not expected to arm themselves with missiles and bombers. But today, the private sector is taking more of its security into its own hands, both defensively and, perhaps, offensively. In

1. U.S. Department of Defense, "The DoD Cyber Strategy," April 2015. (http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf)
2. Commission on Enhancing National Cybersecurity, "Report on Securing and Growing the Digital Economy," December 1, 2016. (https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf)
3. The White House, "National Security Strategy of the United States of America," December 2017, pages 12-13. (https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf)
4. The White House, "National Security Strategy of the United States of America," December 2017, page 21. (https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf)
5. The White House, "National Cyber Strategy of the United States of America," September 2018, page 1 (https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf)
6. U.S. Department of Defense, "2018 Department of Defense Cyber Strategy," September 2018, page 3. (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF)

2016, the U.S. government spent $28 billion on cyber, according to unclassified reports,[7] while the U.S. private sector spent $54.8 billion.[8]

The revolutionary change that nuclear weapons presented to early Cold War strategic thinkers provides relevant parallels to today's technological cyber innovations. How the U.S. government organized itself then can help inform how Washington organizes itself today to prevail in this new battlespace. This paper offers critical lessons from the creation of the early nuclear "Single Integrated Operation Plan" as a path forward to begin to answer some of the same crucial questions that our predecessors asked more than 50 years ago: what targets should be considered and how they should be evaluated; what capabilities need to be developed and deployed to reach those targets; how inter-service rivalry should be minimized to ensure a smooth implantation of the strategy; and what the proper role of allies is.

Congress has repeatedly expressed frustration at the lack of an overarching strategy and doctrine for cyber warfare.[9] To help remedy perceived deficiencies in cyber strategy and planning, the 2019 National Defense Authorization Act included a provision establishing a "Cyberspace Solarium Commission,"[10] modeled after President Eisenhower's 1953 Solarium Commission, to develop America's foundational strategies that Washington implemented throughout the Cold War. As a member of the new Cyberspace Solarium Commission, I commend Brian Mazanec for offering this impressive analysis. The new commissioners and I would be wise to study its findings and draw conclusions about how to begin to assess the strategies ranging from deterrence to norms-based regimes to persistent engagement put before us by Congress.[11]

The goal of any strategist is not the eradication of all surprise in warfare; that would be an unrealistic and unattainable objective. Cold War thinker Thomas Schelling once wrote that surprise happens because of not only "contingencies that occur to no one, but also those that everyone assumes somebody else is taking care of."[12] The nuclear SIOP not only addressed the latter scenario by clarifying what military capabilities the U.S. military would use to target which Soviet assets. Rather, it also provided a roadmap for decision-makers, thus mitigating possible additional crises that would most likely occur as a result of surprises.

This paper does not provide the overarching framework for defending against and prosecuting cyber warfare and cyber-enabled economic warfare. Rather, Mazanec's analysis offers the best path forward for organizing the effort to make those decisions. Our adversaries are already engaged in persistent attacks against our economy and our national security, but our history is replete with examples of how American ingenuity and strategic thinking helped our country overcome overwhelming challenges. We must remember that history and let its lessons guide us into a new and challenging era of warfare.

---

7. Adam Stone, "How much does federal government spend on cybersecurity?," *Fifth Domain*, September 1, 2017. (https://www.fifthdomain.com/civilian/2017/09/01/how-much-does-federal-government-spend-on-cybersecurity)

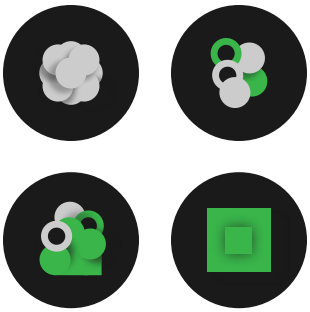
8. "Spending on cybersecurity in the United States from 2010 to 2018 (in billion U.S. dollars)," *The Statistics Portal*, accessed January 2, 2019. (https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/)

9. Morgan Chalfant, "Senators demand cyber deterrence strategy from Trump," *The Hill*, March 8, 2018. (http://thehill.com/policy/cybersecurity/377410-lawmakers-demand-cyber-deterrence-strategy-from-trump); Peter Feaver and Will Inboden, "Washington Needs a New Solarium Project To Counter Cyberthreats," *Foreign Policy*, **June** 26, 2018. (https://foreignpolicy.com/2018/06/26/washington-needs-a-new-solarium-project-to-counter-cyberthreats)

10. Office of Senator Ben Sasse, Press Release, "Senate's Defense Bill Includes Sasse's Cybersecurity Solarium Commission," May 24, 2018. (https://www.sasse.senate.gov/public/index.cfm/press-releases?ID=A75F324A-F7DC-41DE-A0FC-80A472933A28)

11. Annie Fixler and Tyler Stapleton, "Prevailing in Today's Cyber Battlefield Requires Strategic Consensus," *The National Interest*, September 4, 2018. (https://nationalinterest.org/feature/prevailing-today%E2%80%99s-cyber-battlefield-requires-strategic-consensus-30157)

12. Thomas Schelling, foreword to *Pearl Harbor: Warning and Decision*, by Roberta Wolhstetter (Stanford University Press 1962), page viii.



Introduction

In today's national security threat space, nowhere is a dialogue on technology, strategy, and planning more needed than within the cyber realm. Cyber conflict is growing because, thanks to new technologies, opportunities are rapidly expanding. Feasibility barriers are relatively low, and potential asymmetric gains are enormous. As with other, earlier advances in science and industry – from catapults to gunpowder – technological change nearly always precedes the emergence of foundational theoretical strategy. When President Truman employed nuclear weapons against the Japanese, there was no well-developed plan on how these weapons would be used to shape America's future beyond the end of World War II. Seventy years ago, theory, strategy, and planning for nuclear warfare had to develop and catch up to the technological breakthroughs. Today, we are at a similar precipice. We must urgently formulate theories and strategies in the face of today's emerging digital weapons.[13] We can do so more efficiently and effectively by learning more about the processes associated with prior emerging technologies.

One mechanism to address the challenge of deterring,[14] contesting, thwarting, or defending against cyber aggression may be through an operationalized plan akin to the Cold War's *Single Integrated Operational Plan* (SIOP).[15] The SIOP was a detailed blueprint for nuclear war. It included not only what targets were to be attacked, by what nuclear forces, and with what delivery systems, but also the routes and timing of the

13. It is important to recognize at the outset that the analogy of the nuclear experience is not perfect when applied to cyber. There are key differences – such as the role of the private sector – that will be highlighted throughout this monograph. Some cyber scholars, such as Richard Harknett and Robert "Jake" Bebber, have argued that because cyberspace is an entirely new strategic environment with many unique elements, pursuing cyber deterrence is the wrong approach. Instead, concepts such as Bebber's "cyber initiative" (the operational outcome of effectively anticipating the exploitation of cyber-related vulnerabilities) or "cyber persistence" (a strategy of constantly engaging adversaries in cyberspace to observe, disrupt, and disable) is offered as a more appropriate strategic pursuit. Harknett goes so far as to refer to cyber deterrence as a "fool's errand" and argues for a need to escape the deterrence "cul-de-sac." Regardless, the exercise of planning can help resolve these key questions with the benefit of lessons found in the nuclear experience. Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis*, 2017, pages 381-393. (https://doi.org/10.1016/j.orbis.2017.05.003); Robert Bebber, "There is No Such Thing as Cyber Deterrence. Please Stop," *The Cipher Brief*, April 1, 2018. (https://www.thecipherbrief.com/column/strategic-view/no-thing-cyber-deterrence-please-stop); "Hearing to Receive Testimony on the Department of Defense's Role in Protecting Democratic Elections," *Hearing before the Senate Armed Services Subcommittee on Cybersecurity*, February 13, 2018. (https://www.armed-services.senate.gov/imo/media/doc/18-13_02-13-18.pdf)

14. Deterring all forms of cyber aggression is likely impossible. A discussion of deterrence theory and cyber is included in Appendix II.

15. A key challenge for the highly classified nuclear SIOPs, as well as any prospective cyber SIOP, is in signaling to allies and adversaries. With nuclear war planning, visible changes in force structure occurred, which helped with signaling, but cyber force structure or capability changes may not be similarly visible. For more on this issue, see: Adam Segal, "The 'Known Unknowns' of Russian Cyber Signaling," *Council on Foreign Relations*, April 2, 2018. (https://www.cfr.org/blog/known-unknowns-russian-cyber-signaling)

attack and the expected level of target damage.[16] Appendix I provides an overview of the development of SIOPs.

While cyber scholars have long focused on the challenge of applying deterrence theory to cyber conflict,[17] few scholars have focused on the tactical and operational issues associated with applying deterrence theory in practice – namely, the nuclear SIOP experience – to the cyber problem set.[18] Appendix II supplies an overview of deterrence theory and the challenges of applying it to cyberspace.

The exception is Austin Long's March 2017 article, *A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning*.[19] Long's article highlights the value of moving beyond solely theoretical analysis to focus on operational issues, such as planning, targeting, and command and control. This paper builds on Long's analysis by offering additional lessons learned from the SIOP experience. In particular, early nuclear planning processes offer the most salient lessons for the development of a SIOP for cyber conflict, because these documents had to grapple with the most fundamental questions of this new form of conflict, akin to the challenges today's cyber theorists and war planners must tackle.

There was nothing akin to the SIOP before the nuclear era because, historically, war unfolded slowly and the achievement of strategic objectives involved extended campaigns to defeat the other side's military forces. Nuclear weapons, especially when paired with ballistic missiles, changed that. Strategic objectives – such as the destruction of the war-making capacity of an enemy, the collapse of its resistance, and even the annihilation of its population – could be achieved in mere minutes with nuclear war. One's own strategic nuclear forces and the means of controlling them were also at risk. Speed, pre-planned options, a transparent posture of readiness, and declared intentions were critical.

16. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, page 24. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf)

17. For example, see: Martin Libicki, *Cyber Deterrence and Cyber War* (Santa Monica: RAND Corporation, 2009). (https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf); Joseph Nye, "Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly*, Winter 2011. (https://dash.harvard.edu/bitstream/handle/1/8052146/Nye-NuclearLessons.pdf); Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Oxford: Oxford University Press, 2017); Emily Goldman and John Arquilla, eds, *Cyber Analogies* (Monterey, CA: Naval Postgraduate School, 2014). (https://calhoun.nps.edu/bitstream/handle/10945/40037/NPS-DA-14-001.pdf?sequence=1&isAllowed=y); U.S. Department of Defense, Defense Science Board, Report of the Task Force on Cyber Deterrence, February 2017. (http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf); Joseph Nye, "Deterrence and Dissuasion in Cyberspace," *International Security*, Winter 2016/17. (https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266)

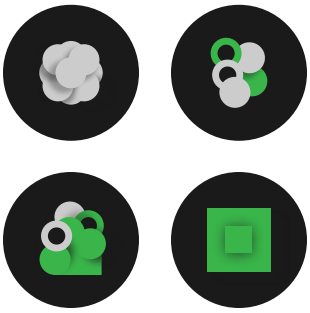
18. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities," *National Research Council of the National Academies*, 2009, pages 183-184. (https://www.nap.edu/read/12651/chapter/1)

19. Austin Long, "A cyber SIOP? Operational considerations for strategic offensive cyber planning," *Journal of Cybersecurity*, March 1, 2017. (https://doi.org/10.1093/cybsec/tyw016)

Cyber conflict is similar. The approximately 30 minutes it takes a ballistic missile to reach its target seems like forever compared to a speed-of-light cyber attack. Cyber strikes on critical infrastructure are, in fact, a lot like strategic nuclear attacks. They can achieve strategic objectives instantly at the outset of a war without having to first engage and defeat armies, navies, and air forces. Furthermore, defense against strategic cyber attacks on critical infrastructure is conceivable in principle, but as of now, that capability is very limited. This too is similar to the situation early in the nuclear era, when large-scale missile and air defense was not achievable.

Many of the factors that prompted the need for the nuclear SIOP are once again at play within the cyber realm: unclear information on what is an effective target, competition within the U.S. government's bureaucracy as to who should carry out the targeting, and the role of allies in the endeavor. With the SIOP, strategic nuclear targeting required constant attention as targets changed, new ones appeared, and defenses evolved. Again, cyber planning shares some similarities. It can take months or years to set in place back doors to take down a cyber target, and that capability is fragile. Regular, standard updates to computer networks can compromise an attack capability, necessitating a careful, deliberate planning process to choose targets wisely ahead of a conflict.

There are valuable process lessons for Washington's approach to deterring, contesting, and defending against cyber aggression from the nuclear SIOPs in the early nuclear era, specifically in the four areas of: (1) the planning process; (2) targeting; (3) force structure and capability requirements; and (4) allied engagement.[20] This monograph looks back at the process of developing the various early SIOPs with an eye toward how they can inform the strategy of another world-changing technology.



Relevant Historical Factors Precipitating The Need for A Cyber SIOP-Like Process

The 1950s planners needed a process to force and facilitate the U.S. government's effort to consider all aspects of nuclear war, including strategy, doctrine, and deterrence theory. Today, while it may be possible to attack certain adversary cyber forces and preempt or disrupt an attack, cyber attacks alone do not kill the cyber operators, and the adversary's replacement tools are readily available. Counterforce concepts appear to have limited potential, and the United States may need to rely on a doctrine of strategic deterrence against crippling critical infrastructure attacks by threatening retaliation in kind – a cyber version of mutually assured destruction – even while recognizing that deterrence theory has imperfect applications in cyberspace (see Appendix II). Washington also needs a range of lesser warfighting options, analogous to Limited Nuclear Options,

20. For the purposes of this study, the primary focus is on the "early nuclear era," defined as 1945 through SIOP-64, which was completed in 1964 and remained in effect into 1966. As appropriate, some more contemporary historical issues will be discussed.

including counterforce options and options to target command and control. The process of developing a SIOP-like plan would allow planners to begin to answer the questions.

The closest thing the U.S. government has to a cyber SIOP today is somewhat similar to the Truman administration's Joint Emergency War Plan of 1948. The Defense Advanced Research Projects Agency's (DARPA) Plan X[21] is a "foundational" cyber warfare program to help the department plan for, conduct, and assess cyber warfare in a manner similar to kinetic warfare.[22] Elements of the program include creating more resilient operating systems and mapping cyberspace to help with target identification.[23] However, just as the Eisenhower administration determined that Truman's planning was insufficient and thus began the SIOP planning process, so too are today's strategic thinkers faced with incomplete planning.

Both nuclear confrontation and today's cyber domain entail offense-dominated operations. While the U.S. government explored and invested in civil defense and air/missile defense, these did not prove feasible or effective at changing the basic conflict outcomes. Defense Science Board assessments conclude that adequate defense of critical infrastructure against a cyber operation by a determined peer adversary is not feasible for the foreseeable future.[24]

Nuclear war – especially facilitated by intercontinental missiles – required precise planning, and the execution had to be rapid. Forces and national command and control were potentially vulnerable, and decision time was measured in minutes due to missile flight times. In worst-case scenarios, the United States faces a similar situation today in the cyber domain. But even if the president need not always act in seconds or minutes in response to a cyber attack, the president still needs options on hand that can be executed with some degree of expeditiousness.

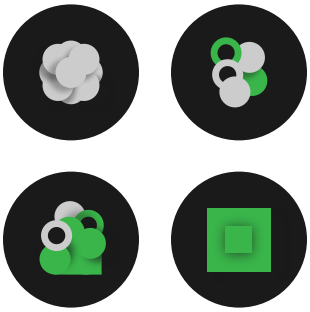
At the same time, it takes months if not years to engineer a cyberattack capability. Historically, strategic targets for nuclear attack were fixed, and operations could be pre-planned in detail. Cyber targets must also be pre-planned and meticulously maintained, although this could change in the future if cyberattack capabilities become more generically applicable, allowing quick ad hoc prosecution. However, committing to a prioritized target is inescapable.

---

21. Ellen Nakashima, "With Plan X, Pentagon seeks to spread U.S. military might to cyberspace," *The Washington Post*, May 30, 2012. (https://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html)
22. U.S. Department of Defense, Defense Advanced Research Projects Agency, "Plan X," accessed January 2, 2019. (https://www.darpa.mil/program/plan-x)
23. Ellen Nakashima, "With Plan X, Pentagon seeks to spread U.S. military might to cyberspace," *The Washington Post*, May 30, 2012. (https://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html)
24. The DSB does, however, conclude that defense against lesser powers, such as Iran and North Korea, may be feasible and highly desirable, justifying substantial expenditures and effort. "Task Force on Cyber as a Strategic Capability," *Defense Science Board*, June 2018. (https://apps.dtic.mil/dtic/tr/fulltext/u2/1055883.pdf)

In the early 1960s, the nuclear SIOP's rigorous planning process exposed assumptions and revealed weaknesses in logic and capabilities. Today, the U.S. government does not fully know – but must urgently determine – what resources it will require to constantly hold at risk a coherent set of cyber targets of major adversaries.

The mere existence of the SIOP sent a powerful deterrent message to adversaries that the United States was serious, had prepared for the unthinkable, and was prepared to act. It signaled that retaliation was inevitable and would be effective. While the existence of a Cyber SIOP would not tell U.S. adversaries the specific targets on U.S. government lists or how Washington intends to attack, adversaries would be keenly aware that things they value would be in jeopardy.



Planning Process Lessons

In 1946, with the advent of nuclear weapons and strategic delivery systems, the national security apparatus found existing planning processes inadequate and saw the need to develop new ones. The first efforts to better integrate the nuclear war planning process entailed the Joint Chiefs of Staff's (JCS) consolidation of Strategic Air Command (SAC) forces under its operational authority in 1946. This is roughly analogous to the Obama administration's purported consolidation of operational control of offensive cyber weapons within the White House. The Trump administration reportedly reversed this consolidation and delegated authorities back to battlefield commanders.[25] The 1946 consolidation enabled the SAC to focus on its primary mission of identifying strategic Soviet targets beyond simply stopping Soviet advances into Western Europe. Then, in 1952, the JCS took additional steps to improve coordination of U.S. nuclear forces through the creation of Joint Coordination Centers (JCCs) for the European and Pacific theaters.[26] However, these JCCs were geared toward operational coordination after hostilities began and did not address pre-hostilities coordination. In 1954, the JCS began to address pre-war coordination by asking each commander to submit a nuclear annex to his respective war plan. In 1958, World-Wide Coordination Conferences began to integrate nuclear plans and target lists.[27]

Integrating Participants through Framing Questions and Organizational Structures

While these mechanisms reduced duplication, the efforts did not achieve true unity of effort. The Air Force then took a leading role in proposing a unified U.S. Strategic Command (including subordinate units responsible for Air Force and Navy Polaris

25. Ellen Nakashima, "Trump gives the military more latitude to use offensive cyber tools against adversaries," *The Washington Post*, August 16, 2018. (https://www.washingtonpost.com/world/national-security/trump-gives-the-military-more-latitude-to-use-offensive-cyber-tools-against-adversaries/2018/08/16/75f7a100-a160-11e8-8e87-c869fe70a721_story.html)
26. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, page 2. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf)
27. Ibid, page 3.

strategic weapon systems). The other military services opposed this plan. The JCS chairman, General Nathan F. Twining, ultimately offered an organizational solution. He reasoned that addressing these two issues would also address the issue of control of strategic forces.[28] The chairman's proposal called for creating a National Strategic Target List (NSTL) and a SIOP, which would address the lack of a "single integrated operational plan." This was documented in an August 1959 note by the secretaries to the JCS on target coordination and associated problems.[29] To help further frame the key issues, in 1959 General Twining also posed 18 questions in four general areas to the various stakeholders, identified in Table 1 below.

Table 1: JCS Chairman Questions to Frame Key Issues for SIOP Development[30]

On targeting policy
1. What should it be?
2. What categories of target should it cover?
3. What agency should develop it? Maintain it?
4. What agency should review and approve the policy?
On an integrated operational plan
1. Do we need such a plan?
2. What agency should develop it? Review and approve it?
3. Should non-all-weather systems attack strategic targets? If so, under what conditions?
4. Should carrier forces have H Hour strategic targets?
5. If carrier forces are relieved of strategic targets, how do we state their nuclear mission?
6. Is there an immediate need for a Unified Strategic Command?
7. Is a Unified Strategic Command desirable in the future?
8. If we do not form a unified command now, should POLARIS and SAC Plans be integrated?
9. If so, how?
On operational control of the nuclear strike forces
1. Should unified commanders have H Hour strategic targets?
2. Should Joint War Room Annexes and Joint Coordination Centers be continued?
3. What additional measures would improve coordination?
Questions 17 and 18 pertained to operational analysis and war gaming

28. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, pages 5-6. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf)
29. Memo by the Secretaries to the Joint Chiefs of Staff, "Target Coordination and Associated Problems," August 17, 1959. (https://nsarchive2.gwu.edu/NSAEBB/NSAEBB130/SIOP-2.pdf)
30. Scott D. Sagan, "SIOP-62: The Nuclear War Plan Briefing to President Kennedy," *International Security*, Summer 1987, pages 22-51. (http://www.jstor.org/stable/2538916)

CYBER APPLICATION

As with Twining's questionnaire, it is likely that various agencies (U.S. Cyber Command, National Security Agency, Central Intelligence Agency, Department of Homeland Security, Geographic Combatant Commanders, and others) would again be unwilling to cede their respective authority and, despite the number of existing joint cyber forces currently in existence, new organizational compromises will be necessary.

While U.S. Cyber Command has been established as a unified command within the Department of Defense, it may be helpful to integrate interagency and possibly private-sector participants through an integrated interagency organization – for targeting and other purposes, as appropriate.

While the participants initially attempted to answer the chairman's questions jointly, there were "conceptual differences."[31] Separate responses were ultimately submitted, and General Twining concluded that "not much more progress can be achieved under the present arrangements."[32]

Taking into account the ongoing service rivalries and divergent perspectives that had led to the need for the questionnaire in the first place, General Twining then proposed a national strategic targeting policy. In August 1960, Secretary of Defense Thomas Gates ultimately approved an organizational compromise that designated the SAC commander as director of strategic target planning (dual-hatted with existing SAC responsibilities), as well as the creation of a Joint Strategic Target Planning Staff (JSTPS).[33]

The JSTPS was relatively small (around 300 billets initially) but included staff from all key stakeholders in the military services and theater commands. The JSTPS staff would later be reduced to around 180 after SIOP 62.[34] The JSTPS had two main organizations, one dedicated to developing the NSTL and the other the SIOP, as depicted in Figure 1 below.

Figure 1: JSTPS Organization[35]

31. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, page 9. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf)
32. Ibid.
33. Peter Pringle and William Arkin, SIOP: *The Secret U.S. Plan for Nuclear War* (New York: Norton and Company, 1983), page 112; Memo from the Secretary of Defense for the Joint Chiefs of Staff Chairman, "Target Coordination and Associated Problems," August 16, 1960 (B-76590).
34. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Revisions 1-8 to SIOP 64," page 58.
35. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, page 13. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf)

The Senior Liaison Representatives group served as the formal liaisons to and representatives from the various stakeholder groups (military services, JCS, unified commands, etc.). A Policy Committee also served a key function of reviewing and approving policy and adjudicating policy disputes. The two key production units – the NSTL Division and the SIOP Division – were staffed differently. There were disputes over representation in the new organization – with some advocating for equal representation and others proportionate to the nuclear forces committed to the SIOP. The NSTS was staffed with the best qualified officers, regardless of service, while the SIOP Division was staffed proportional to the forces each service provided for the execution of the SIOP. The staff had four months to develop the first SIOP, SIOP 62.

Another area of disagreement with the new JSTPS was the intelligence function. The chief of naval operations recommended the organization have an intelligence panel, including Department of Defense intelligence officers, as well as staff from the CIA. The director of strategic target planning challenged the need for this intelligence panel because he believed he had adequate resources already. But he did add 10 personnel to help improve intelligence coordination.[36] According to Peter Pringle and William Arkin, over time, SAC became "not only a major consumer but also a dominant, if largely unnoticed, operator in strategic intelligence."[37] By the early 1990s, the Air Force's 544th Aerospace Reconnaissance Technical Wing, SAC's primary intelligence unit, had grown to over 1,000 personnel and was the largest intelligence arm of the Air Force. In the following two decades, SAC helped restructure intelligence collection with the aim of preparing and implementing the SIOP.[38] It was ultimately SAC's Directorate of Intelligence that produced the first working target list that served as the first National Strategic Target Data Base (NSTDB), with about 4,000 targets.[39] In fact, many of the procedures and staff processes used by the new JSTPS closely resembled those developed by SAC.[40]

In addition to the government stakeholders, the RAND Corporation also helped develop the intellectual ecosystem that offered critical concepts, such as the need for survivable forces and the concept of counterforce targeting.[41] These provided the theoretical foundation upon which the JSTPS operated. RAND scientists also served

CYBER APPLICATION

Ensuring adequate resources for the gathering and assessing of adversarial cyber science and technical intelligence (S&TI), Human Intelligence (HUMINT), and Signals Intelligence (SIGINT) is critical for enabling the continued effectiveness of a targeting strategy. S&TI is particularly important because almost any change to network configuration could eliminate an attack capability against a target on that network. Thus, it is imperative to maintain constant vigilance on target sets to ensure operational success.

Private-sector and government efforts to develop a theory of cyber and employment policies are underway, but efforts should expand. Consideration can be given to whether there should be a Federally Funded Research and Development Center for cyber, focused exclusively on strategy, doctrine, and policy for the use of cyber weapons.

36. Ibid, pages 16-17.
37. Peter Pringle and William Arkin, *SIOP: The Secret U.S. Plan for Nuclear War* (New York: Norton and Company, 1983), page 70.
38. Michael Meridith, "Strategic Command Intelligence Role Echoes Its Past," *Air Force News*, June 23, 1999. (https://fas.org/irp/news/1999/06/n19990623_991226.htm)
39. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, page 18. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf); United States General Accounting Office, "Strategic Weapons: Nuclear Weapons Targeting Process," September 27, 1991, page 10. (http://www.gao.gov/assets/90/89136.pdf)
40. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 64, Volume I Narrative," page 4. (https://archive.org/details/HistoryoftheJointStrategicPlanningStaffPreparationofSIOP64)
41. Andrew May, "The RAND Corporation and the Dynamics of American Strategic Thought, 1946-1962," Doctoral Dissertation, August 6, 1998, page 7.

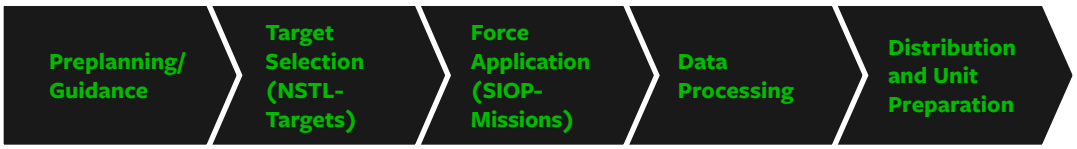
in key government positions, helping further cultivate the connective tissue between government and the scholarly community.

The JSTPS also produced documents beyond the SIOP, such as employment policy (later called the Nuclear Weapons Employment Policy), the Nuclear Reconnaissance List, and the Airborne SIOP Reconnaissance Plan. While outside the scope of this paper, which focuses on the early nuclear era through SIOP 64, the JSTPS in 1968 began convening a Scientific Advisory Group with experts from industry, academia, and government.[42] Such an effort could merit further study for the formation of a military-industrial-cyber complex.

Using a Sequential and Interdependent Process with Capability Cutoff

The JSTPS's two production units worked in tandem, producing first the NSTL in the target division, while the SIOP Division worked to apply forces to the targets. This was followed by data processing, and ultimately approval and distribution of the SIOP, as depicted in Figure 2 below.

Figure 2: SIOP Development Process



The SIOP production team then led the distribution and unit preparation phase, which included the development and dissemination of specific strike timing and other supporting materials. Beginning with SIOP 62, a capability cutoff (i.e., only existing or planned near-term capabilities were incorporated into the process) was used to account for ever-evolving capabilities and the need to conclude a static (albeit iterative) planning process. Forces were committed to the SIOP (and thus targets from the NSTL). Constraints were also considered as part of this process. For example, with SIOP 62 there was a "Fallout Constraint Policy" that limited some strike options.[43] Before force application could occur, the SIOP Division conducted a robust evaluation of forces consisting of the application of committed SIOP forces (Phase 1) and the application of supporting theater forces (Phase 2).[44]

CYBER APPLICATION

With cyber weapons, it is even more critical to address the capability cutoff issue, since weapons and targets are perishable, negating capabilities quickly. More dynamic planning will be necessary as technology maturation is continual and exponential. Additionally, cyber weapons and targets may require additional planning filters – such as allowing for time to develop "back doors" for targets.

42. James T. Pratt, "Strategic Target Planning and the JSTPS," *U.S. Army War College*, March 1988, page 6 & 11. (http://www.dtic.mil/dtic/tr/fulltext/u2/a195083.pdf)
43. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, pages 20-23. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf)
44. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964, page 20. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)

Another aspect of this process was the assessments made during the numerous SIOP iterations. These assessments varied between formal studies, led by the JCS or JSTPS, and less formal ones, such as President Eisenhower's Special Assistant for Science and Technology Dr. G.B. Kistiakowsky's assessment of SIOP 62.[45] This general planning process did not change from SIOP 62 through all eight revisions of SIOP 64.[46]

Increasing Information Needed to Drive Planning

In general, SIOP planning was based on the development of a cascading hierarchical guidance flowing from presidential directives (or their historical equivalent) to other nuclear force employment guidance, and eventually the SIOPs themselves.[47] The National Strategic Targeting and Attack Policy promulgated by the JCS was key in providing the guidance for developing SIOP 62.[48] Future iterations of the SIOP used updated versions of this and other detailed guidance from JCS.[49]

More detailed guidance required more time to interpret. The first two months of SIOP 63's development were focused on interpreting – through the Policy Committee – what the guidance meant.[50] There were numerous technical areas requiring clarification or resolution, such as how to define "alert forces," what operational factors (weather, weapon reliability, etc.) should be taken into consideration, and if destruction before launch (essentially pre-launch survivability) was intended to be applied. Destruction before launch helped calculate what forces would be available to respond to an unexpected attack.

The Red Planning Board's adversarial plans known as the Red Integrated Strategic Offensive Plan were important tools used to "wargame" and test the SIOPs.[51] As soon as SIOP 62 entered into force, war gaming to evaluate the effectiveness of the plan and inform future SIOPs began.[52] The SIOP Division led these games. While some

CYBER APPLICATION

Cyber weapons-planning may require even more intervals and updates, given the transitory and perishable nature of cyber weapons and targets. A cyber SIOP would require frequent revisions.

High-level cyber guidance can help set the stage for a cyber SIOP and could be informed by the nuclear SIOP processes.

45. Ibid, page 2.
46. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Revisions 1-8 to SIOP 64," page 1. (https://archive.org/details/HistoryoftheJointStrategicPlanningStaffPreparationofSIOP64)
47. U.S. Government Accountability Office, "Strategic Weapons: Changes in the Nuclear Weapons Targeting Process Since 1991," July 31, 2012, page 5. (http://www.gao.gov/assets/600/593142.pdf)
48. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, page 18. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf)
49. Joint Chiefs of Staff, "Guidance for the Preparation of the Single Integrated Operational Plan – 1963 (SIOP 63)," August 18, 1961; U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964, page 4. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)
50. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964, page 18. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)
51. Hans Kristensen, "The RISOP is Dead – Long Live RISOP-like Nuclear Planning," *Federation of American Scientists*, July 21, 2008. (https://fas.org/blogs/security/2008/07/risop/)
52. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964, page 10. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)

CYBER APPLICATION

A Red Planning Board for cyber could prove equally useful for cyber planners.

Technical assumptions are even more critical with cyber operations, given the unique interdependence between weapon and target. Thus, developing clear planning factors is essential.

Developing an adversary cyber plan may be useful in war-gaming any cyber SIOP. However, due to the cross-domain nature of cyber operations, such an adversary plan may need to include non-cyber means, as well. A cyber Red Integrated Strategic Offensive Plan concept merits more examination.

The integration challenge for cyber is an issue not just for the military services and unified commands, but instead across the various Cyber Mission Forces of U.S. Cyber Command (especially the National Mission Force) and with the other key cyber actors across the interagency.

controversy ensued (largely over who participated), these war games proved informative to the SIOP's continued development.[53]

SIOP planners wrestled with how to factor in technical concerns and assumptions. For example, with SIOP 62, planning factors assumed that weather was unlikely to have significant adverse effects on accuracy of weapon delivery – perhaps an overly optimistic assumption.[54]

Other planning factors included the "assurance factor" associated with the probability of neutralizing a target. The SAC Commander called for a 97 percent assurance factor for the development of SIOP 62, which some thought too high.[55] By SIOP 64, key planning factors were refined, and there were sophisticated mathematical formulas associated with pre-launch survivability, weapon system reliability, weather darkness factor, and penetration probability.[56] Entities such as the Weapons Systems Evaluation Group conducted additional analysis to inform decisions on other planning factors.[57] Development of SIOP 63 also introduced time for target drills to help achieve a more effective plan.

Achieving consensus on planning factors, clarity on overall employment guidance, and a good understanding of likely adversary plans (Red Integrated Strategic Offensive Plan) were all essential for the SIOP planning process, especially as the process became more complex over time. For example, producing SIOP 63 required around 8,000 documents, and by 1963 the production of SIOP 64 required around 15,000 documents.[58]

Targeting Lessons

The SIOP planning addressed, *inter alia*, the process of selecting and prioritizing targets. Prior to this point, the process of nuclear targeting was largely decentralized and duplicative across the military services and unified commands.

Integrating Targeting and Developing Consistent Target Categories and Approaches

To address the fragmented targeting activities among the military services, the National Security Targeting Data Base served as the foundation for more refined and integrated

53. For example, the early SIOP 62 war games led by the Navy included civilian organizations not normally involved in such games.
54. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, page 26. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf)
55. Ibid, page 28; William Burr, "New Evidence on the Origins of Overkill," *National Security Archive*, November 21, 2007. (https://nsarchive2.gwu.edu/nukevault/ebb236/)
56. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Revisions 1-8 to SIOP 64," page 10. (https://archive.org/details/HistoryoftheJointStrategicPlanningStaffPreparationofSIOP64)
57. Andrew May, "The RAND Corporation and the Dynamics of American Strategic Thought, 1946-1962," Doctoral Dissertation, August 6, 1998, page 371.
58. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Revisions 1-8 to SIOP 64," page 58. (https://archive.org/details/HistoryoftheJointStrategicPlanningStaffPreparationofSIOP64)

targeting. It represented the best information available to U.S. intelligence agencies at the time.[59] The NSTDB was built using various sources, but the primary contributor was the Air Force's Target Data Inventory, developed in consultation with the Army and Navy.[60] From the NSTDB, the planning staff then developed the NSTL, the narrower, priority target list. Once the NSTL was developed, each target (a desired ground zero) was assigned to a specific task relative to the destruction of the target. The NSTL Division then provided the SIOP Division with a prioritized list in order to begin planning for force application (i.e., detailed mission planning).

In addition to establishing an integrated database of potential targets and then a prioritized target list, JSTPS staff had to grapple with refining or defining some target categories and approaches.[61] These operational targeting debates were distinct from deterrence theory debates about how many targets were adequate for minimum deterrence.[62] (For a discussion of the applicability of deterrence theory to cyber, see Appendix II.)

For SIOP 62, targets fell into three main groups: The first group contained the targets whose assured destruction would meet specific objectives in the overarching targeting policy. The second group contained the targets whose destruction was necessary to be able to destroy the targets in the first group. And finally, the third group contained targets senior leaders believed should be attacked because they would be significantly damaged due to co-location.[63] Within these groups of targets, there were four broad categories: Soviet nuclear forces and supporting command and control; military and political leadership; other military forces; and war-supporting industrial and economic activities. In developing the NSTL that covered these groups of targets, there was debate, particularly for the early SIOPs, regarding whether a maximum or minimum level of damage should be inflicted. The SIOP 63 targeting guidance avoided wading into this debate by calling for the use of forces to "maximize the achievement of the objectives of the plan," rather than setting specific minimum or maximum damage levels.[64] From 1960 to 1974, the targets were ranked in order of priority: (1) urban-industrial; (2) nuclear forces; (3) other military forces. This ranking did not necessarily reflect the order of battle.

59. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, page 19. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf)
60. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964, page 18-19. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)
61. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, page 26. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf)
62. Andrew May, "The RAND Corporation and the Dynamics of American Strategic Thought, 1946-1962," Doctoral Dissertation, August 6, 1998, page 221.
63. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, page 24. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf)
64. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964, page 16. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)

CYBER APPLICATION

Given that the range of cyber targets (tactical to strategic) is nearly infinite, a key task for a cyber SIOP would be to determine the target threshold (of strategic significance) and the appropriate target groups for a National Strategic Cyber Target Database and National Strategic Cyber Target List. Additionally, a cyber target list will change frequently because targets may appear and disappear or change function depending on its programming. There are parallels to the planning for mobile nuclear targets. Finally, the database may also need to include cyber targets in neutral and friendly nations to disable these other networks the adversary may use in its offensive operations.

No such analogous coordination appears to exist for cyber planners today. A National Strategic Cyber Target Database and National Strategic Cyber Target List would help address this challenge.

Growing Intelligence Needed to Support Targeting

Although the JCS decided against an independent intelligence advisory board, SIOP development required a continuous stream of intelligence. Eventually, the JSTPS began producing the Nuclear Reconnaissance List and SIOP Reconnaissance Plan to help guide intelligence collection efforts and to plan for damage assessments during a nuclear conflict. The president's Foreign Intelligence Advisory Board also played a role in some of these efforts.

During later SIOPs, intelligence collection focused on identifying and reliably locating an adversary's land-mobile and submarine-launched missiles and other relocatable strategic assets. Without accurate intelligence to destroy these assets, the adversary would have a second-strike capability. While many of the early RAND analysts without security clearances believed sufficient intelligence on this topic did not exist and therefore a counterforce strategy was implausible, the U.S. in actuality had reasonably good intelligence on fixed and mobile Soviet targets.[65] (However, the percentage of Soviet assets that could be effectively targeted remains debatable.)[66] Early SAC target data, which formed the basis of the NSTDB, was based on "Project Wringer," a massive effort to debrief individuals repatriated from the Soviet Union.[67] Later, clandestine aerial overflights and early space systems, such as Corona, Gambit and Hexagon, further supplemented this effort.[68]

The CIA was not substantively contributing targeting intelligence, because when the CIA was established, there was a general understanding that the Army, Navy, and Air Force would provide for military intelligence in their respective fields.[69]

Moving Toward Targeting Flexibility and Options

In the 15 iterations of the SIOP, through the last revision of SIOP 64 in 1966, planners introduced significantly greater flexibility in targeting. While SIOP 62 included the option to exempt specific countries from the initial attack, redirect follow-on forces, recall manned systems after initial launch, selective launch of some forces, and dual targets for

CYBER APPLICATION

Cyber operations are much more intelligence-dependent than nuclear operations, and there are often tensions between cyber operations and intelligence over whether to use an exploit or asset in an operation or to retain it for intelligence purposes. Therefore, not only robust intelligence support but also integration and coordination are critical. This must involve the entire intelligence community.

The lack of integration of CIA intelligence during the early SIOPs should not be replicated in today's cyber domain, as information about if and how the senior leadership of the enemy would conduct offensive cyber operations is essential in preventing strategic surprise.

65. Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies*, December 24, 2014, pages 1-2, 38-73, 44. (https://doi.org/10.1080/01402390.2014.958150)
66. Andrew May, "The RAND Corporation and the Dynamics of American Strategic Thought, 1946-1962," Doctoral Dissertation, August 6, 1998, page 257.
67. Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies*, December 24, 2014, pages 1-2, 38-73, 44. (https://doi.org/10.1080/01402390.2014.958150)
68. Robert L. Perry, "A History of Satellite Reconnaissance: The Perry Gambit & Hexagon Histories," *Center for the Study of National Reconnaissance Classics*, November 1973. (http://www.nro.gov/Portals/65/documents/history/csnr/gambhex/Docs/Perry_Gambit_Hexagon_History_single_pages.pdf)
69. Raymond L. Garthoff, "Estimating Soviet Military Intentions and Capabilities," in eds. Gerald K. Haines and Robert E. Leggett, *Watching the Bear: Essays on CIA's Analysis of the Soviet Union* (Central Intelligence Agency, March 2007). (https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/article05.html)

missiles,[70] it was basically designed for execution as a whole and did not have robust segmented options.[71] In fact, some SAC officials argued that anything short of executing the SIOP as a whole would "involve the acceptance of certain grave risks … to the point that … our national survival might not be fulfilled."[72] Proponents of a more rigid plan believed that introducing more options would create confusion and reduce the chances of success. However, the Kennedy administration's preferences for flexibility carried the day.

In developing the guidance for SIOP 63, the deputy secretary of defense called for a wider range of alternatives or options, including options for withholding reserve forces from the initial attack and avoiding attacks on urban-industrial populations, government control centers, and/or one or more Sino-Soviet bloc nation. The JCS's planning objectives implemented this higher-level guidance for SIOP 63 through three overarching tasks and five attack options.[73] These are outlined in Table 2 below.

Table 2: SIOP 63 Tasks and Attack Options[74]

Tasks
1. Destroy or neutralize the military capabilities of the enemy, while retaining ready, effective and controlled U.S. strategic capabilities adequate to assure, to the maximum extent possible, retention of U.S. military superiority to the enemy, or any potential enemies, at any point during or after the war.
2. To minimize damage to the U.S. and its allies, and in all events to limit such damage to a level consistent with national survival and independence.
3. To bring the war to an end on the most advantageous terms for the U.S. and its allies.
Attack Options
1. Execute task 1 under conditions of U.S. pre-emption, but keeping back for possible subsequent use forces programmed for tasks 2 and 3.
2. Execute tasks 1 and 2 under same U.S. pre-emption condition but withholding for possible subsequent use forces programmed for task 3.
3. Execute task 1 under tactical warning but holding back for subsequent use forces programmed for tasks 2 and 3.
4. Execute tasks 1 and 2 under tactical warning but holding back forces for task 3.
5. Execute all three tasks under tactical warning.

CYBER APPLICATION

As cyber weapons are transitory in nature and perishable, it is important to define planning in terms of broader tasks and attack options, some of which were first introduced in the Department of Defense's 2015 Cyber Strategy and remained in the most recent 2018 strategy. As with the nuclear SIOP, these should be broad to allow flexible responses and the application of a range of evolving cyber weapons. Addressing the fleeting nature of cyber weapons will be one of the most difficult tasks of developing a cyber SIOP.

70. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, page 25. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf); U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964, page 6. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)
71. Scott D. Sagan, "SIOP-62: The Nuclear War Plan Briefing to President Kennedy," *International Security*, Summer 1987, page 49. (http://www.jstor.org/stable/2538916)
72. Andrew May, "The RAND Corporation and the Dynamics of American Strategic Thought, 1946-1962," Doctoral Dissertation, August 6, 1998, page 264.
73. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964, pages 5 & 14. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)
74. Ibid, page 14-16.

CYBER APPLICATION

Such flexibility may be difficult to replicate in the interconnected world of cyberspace today. However, a bank of Zero Day vulnerabilities and special cyber weapons could constitute a reserve force capability.

This menu of options introduced more flexibility in SIOP execution and targeting. Beginning with SIOP 63, targets were grouped by task, allowing a greater prioritization of strategic capabilities.[75] SIOP 63 brought counterforce targeting to an operational level and increased the likelihood of achieving deterrence through a second-strike capability.[76] SIOP 63 also introduced the establishment of a reserve force for operations immediately after the initial attack.[77]

Force Structure/Capability Requirements Lessons

As the SIOPs evolved, so too did the theories and strategies of deterrence and a corresponding awareness of the weapons and capabilities needed to prevail in the nuclear age. Issues associated with new nuclear capabilities are what convinced U.S. leadership of the necessity of a SIOP, specifically the questions regarding command and control of the new Fleet Ballistic Missile (Polaris).[78]

Developing Indirect Relationship between Nuclear Planning and Force Structure/Capability Requirements

In the early 1960s, there was no direct linkage between the process of developing the SIOP and the determination of force capability requirements. Rather, it was an informal and indirect, and evolved over time.[79] Targeting focused on weapons available while decisions about the force structure/capability requirements were based on a horizon of five to 10 years. However, planners identified immediate deficiencies in force capabilities. Over time, the planning process revealed the need for diversified and survivable forces to implement second-strike flexibility and the need for improved command and control and warning systems to manage SIOP execution. SIOP forces grew and reached their peak during SIOP 64, Revision 4, which was in effect from January to March 1965. SIOP forces then declined as SAC phased out its medium bomber force and introduced more sophisticated ICBMs with higher weapon system reliability. In contrast, SIOP 62 had at most a negligible role for missile forces.[80]

75. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 64, Volume I Narrative," page 4. (https://archive.org/details/HistoryoftheJointStrategicPlanningStaffPreparationofSIOP64)
76. Andrew May, "The RAND Corporation and the Dynamics of American Strategic Thought, 1946-1962," Doctoral Dissertation, August 6, 1998, page 380.
77. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964, page 9. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)
78. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 64, Volume I Narrative," page 2. (https://archive.org/details/HistoryoftheJointStrategicPlanningStaffPreparationofSIOP64)
79. U.S. General Accounting Office, "Strategic Weapons: Nuclear Weapons Targeting Process," September 27, 1991, page 20. (http://www.gao.gov/assets/90/89136.pdf)
80. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Revisions 1-8 to SIOP 64," pages 18 & 20. (https://archive.org/details/HistoryoftheJointStrategicPlanningStaffPreparationofSIOP64)

Ensuring Planning Was Consistent with Existing and Available Force Structure

When working to increase flexibility in SIOP 63, staff emphasized that it was key to ensure the SIOP did not outpace the actual capacity to execute the plan. Prior to that emphasis, there was likely inadequately centralized command and control to execute some of options in the early SIOPs. At the time, theater commanders determined which of their forces to make available for use under the SIOP and what other forces (beyond SAC and submarine-launched Navy forces) to commit to the SIOP.[81] As a result of decentralized command, components of the early SIOPs may have been impossible to implement.

Allied Engagement Lessons

U.S. nuclear forces and operational plans for their use did not exist in a vacuum. They existed to achieve U.S. national security objectives vis-à-vis the Soviet Union, which included the protection of U.S. allies. As discussed previously, the guidance for SIOP 63 expressly identified minimizing damage (task 2) and bringing the war to an end on advantageous terms (task 3) not only for the U.S. but also its allies. These allies were principally members of the North Atlantic Treaty Organization (NATO).

Growing Allied Role in SIOP Development

There was limited collaboration with allies in the development of the early SIOPs. For example, SIOP 62 excluded the potential usefully Supreme Allied Commander Europe forces because the U.S. did not want to provide the plan to allied governments whose forces were part of NATO and would be utilized in exercising the SIOP.[82] This made it more difficult to assure allies that the U.S. could provide extended deterrence.

Early long-term plans for NATO's nuclear role imagined the creation of a multinational nuclear force with mixed-national crews. While NATO did not create this force, the U.S. did eventually integrate NATO into the SIOP process. Over time, the U.S. deliberately expanded NATO's role in nuclear matters. NATO allies were first brought into the SIOP process with SIOP 64. Indeed, it was a major turning point in allied coordination when DOD officials, in September 1964, briefed SIOP 64 not only to the president but also to the secretary general of NATO. This was done to ensure that allies who were equally reliant on the plan's deterrent effect were aware of policies and capabilities contained in the SIOP.

CYBER APPLICATION

Cyber strategists need to ground planning in existing cyber force capabilities. Unlike the nuclear age, when these capabilities were exclusively held within the Air Force and Navy, today's offensive capabilities are spread throughout the military, intelligence community, and law enforcement. Joint cyber exercises would test the plan's viability, as later nuclear war planning exercises did.

Cyber issues involve a domain that is geographically dispersed, and many cyber operations will necessarily involve network infrastructure in allied, neutral, and adversary nations. Therefore, allies should be integrated into the cyber SIOP planning process.

81. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964, pages 6, 28, & 17. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)

82. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP 62," declassified February 13, 2007, page 20. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-62%20history.pdf)

CYBER APPLICATION

A Cyber Posture Review or other DOD study could examine, inter alia, how Washington should share plans with allies. Given that the private sector is a frontline actor in cyberspace, the United States should also consider whether to share plans with trusted partners in the U.S. and foreign private sectors.

Another major change was the addition of NATO personnel to the JSTPS following an agreement reached at the NATO Ministerial Conference in Ottawa in May 1963. Four NATO officers had continuous access to a wide range of SIOP-related data. SIOP 64 explicitly addressed information-sharing, and planners developed a special version of SIOP 64 for use by NATO military staff agencies. Some information, however, was still deemed too sensitive. [83]

Conclusions and Recommendations

The SIOP represents the culmination of an integrated military effort to determine what targets were to be attacked, by what forces, and in what manner during a nuclear conflict. Many of the factors that led to the need for the nuclear SIOP are now prompting U.S. government efforts to address the strategic cyber threat. To jumpstart the planning process for a cyber SIOP, decision makers should pose questions similar to those offered by General Twining in 1959 to help identify the key questions and challenges. See Table 3 for a draft of these potential framing questions.

Table 3: Potential Questions to Frame Key Issues for Cyber SIOP Development[84]

On cyber targeting policy
1. What should it be?
2. What categories of target should it cover?
3. What agency should develop it? Maintain it?
4. What agency should review and approve the policy?
On an integrated operational plan for major cyber war
1. Do we need such a plan?
2. What agency should develop it? Review and approve it?
3. Should Cyber Combat Mission Force teams and Cyber Protection Force teams have strategic targets or a role in the plan (in addition to Cyber National Mission Force teams)?
4. How does U.S. Cyber Command's elevation from a subordinate unified command to a full Unified Combatant Command impact the planning process?
5. What, if any, changes should be made to U.S. Cyber Command's structure, mission, and authorities, to better enable it facilitate the development of a cyber SIOP?
6. How should other U.S. government cyber forces outside of the Department of Defense be integrated into the U.S. Cyber Command planning effort?

83. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 64, Volume I Narrative, pages 2, 49, 50, 56, 58, & 60-62. (https://archive.org/details/HistoryoftheJointStrategicPlanningStaffPreparationofSIOP64)

84. These questions are developed based on the JCS framing questions from the first nuclear SIOP. Bolding indicates new or modified questions. Scott D. Sagan, "SIOP-62: The Nuclear War Plan Briefing to President Kennedy," *International Security*, Summer 1987, pages 22-51. (http://www.jstor.org/stable/2538916)

On operational control of the strategic cyber strike forces
1. Should Geographic Combatant Commanders have responsibility for strategic targets? How should planners account for geography in cyberspace?
2. What additional measures would improve coordination?
Interagency and non-governmental roles
1. What should be the role of the CIA, Office of the Director of National Intelligence Cyber Threat Intelligence Integration Center, and other IC elements?
2. What is the role of industry and the private sector?
3. What existent plans are relevant and must be integrated – such as unified intelligence strategies, theater campaign plans, etc.?

Interagency coordination and whole-of-government planning is required to prepare for cyber conflict. The roles of the Departments of Defense, State, Treasury, Commerce, Homeland Security, and Energy as well as the intelligence community all need to be reconciled and integrated. Cyber-related interagency stovepipes, resource and personnel battles, and "conceptual differences" will likely be difficult to resolve as the inter-service challenges from the early days of SIOP development.

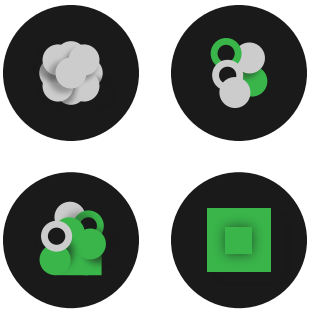
The time required to formulate SIOP 62 should inform decisions regarding the amount of time and resources needed for the first cyber SIOP, as well as the need to establish a similarly iterative planning process. Developing a cyber SIOP will require significant investment of time and energy.

The history of warfare is replete with new technologies that altered the balance of power and the way conflicts were won and lost. The IT revolution has had profoundly positive effects for people, but it has opened the door to new avenues for espionage and damaging attacks.[85] Washington must thwart, defend against, and possibly deter cyber attacks. Even if deterrence proves impossible in some areas of cyber conflict, the process of developing a cyber SIOP will help generate a new strategic framework and delineate the key operational and tactical cyber warfighting issues.[86]

By historical comparison, it is as though we are in the 1950s and early 1960s. We know that these new weapons are game changers, but we have not created an integrated force structure, mapped out their political and military roles, and assessed their impact on statecraft and international politics. It is time to learn from the past and prepare for the future.

85. Many of these are explored in Manuel Castells, *The Information Age: Economy, Society and Culture*, Vol. 1-3. (Oxford: Blackwell, 1996).

86. Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis*, 2017, pages 381-393. (https://doi.org/10.1016/j.orbis.2017.05.003)



Appendix I: Background on Early Nuclear SIOPs

Immediately following World War II, Washington began to grapple with the impact of its nuclear arsenal. At first, despite its exclusive monopoly, the United States pursued a goal of international control of nuclear weapons, recognizing their power and the unique dangers they posed. For a while, a similar period of cyber dominance (or at least tranquility) may have allowed similar assumption of pax-cyber, but that window has closed.

When efforts to seek international control of nuclear weapons failed, the United States established new policies for its nuclear arsenal.[87] For example, President Truman put nuclear weapons under civilian control (the U.S. Atomic Energy Commission) rather than under military control, and reserved sole discretion as to when to employ them.[88] However, the special status afforded to nuclear weapons did not mean the U.S. military was not planning for their use. In June 1948, the U.S. government approved the first nuclear war plan, known as the "Halfmoon" Joint Emergency War Plan, which called for using 50 nuclear weapons against 20 Soviet cities.[89]

The SAC revised the U.S. government's nuclear war plan in 1949. Emergency War Plan 1-49 called for using all 133 nuclear weapons then in the stockpile against 70 Soviet cities.[90] Later SAC war plans were similarly structured, with fewer than 100 targets and an approximately three-week execution period.[91]

As the Soviets developed their own nuclear capability and U.S. nuclear capabilities grew, more serious planning – with an eye toward achieving deterrence – soon began.[92] The process is depicted in Figure 3 below.

---

87. "Declaration on Atomic Bomb by President Truman and Prime Ministers Attlee and King," November 15, 1945, (https://carnegieendowment.org/2005/11/01/nonproliferation-turns-60-pub-17664)

88. Steven Rearden, *History of the Office of the Secretary of Defense: The Formative Years, 1947-1950*, vol. 1 (Historical Office, Office of the Secretary of Defense: Washington DC) page 425-431. (https://history.defense.gov/Portals/70/Documents/secretaryofdefense/OSDSeries_Vol1.pdf) President Eisenhower would partially reverse this special status by giving the military some launch authority, but the special status established by Truman's actions remained.

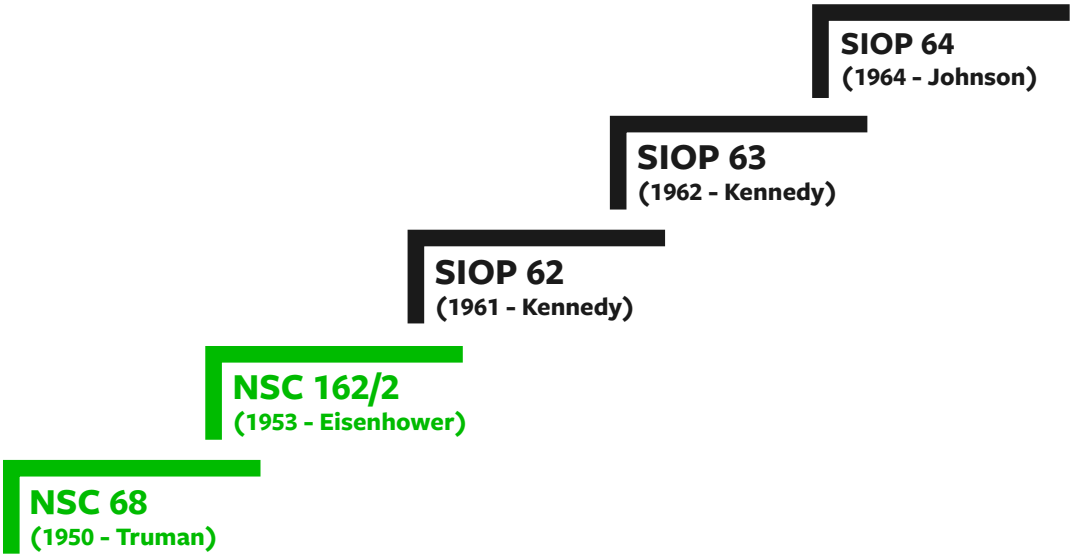
89. Karen J. Weitze, "Cold War Infrastructure for Strategic Air Command: The Bomber Mission," *Air Combat Command*, November 1999. (http://www.usaf-sig.org/index.php/references/reference/114-research-material/552-cold-war-infrastructure-for-strategic-air-command-the-bomber-mission)

90. Tom Engelhardt, *The End of Victory Culture: Cold War America*, (New York: HarperCollins, 2007).

91. James T. Pratt, "Strategic Target Planning and the JSTPS," *U.S. Army War College*, March 1988. (http://www.dtic.mil/dtic/tr/fulltext/u2/a195083.pdf)

92. Herman Kahn, "Nuclear Proliferation and Rules of Retaliation," *Yale Law Journal*, 1966, page 78. (https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=5818&context=ylj)

Figure 3: Key Nuclear War Plans in the Early Nuclear Era



SIOP 62 was relatively short-lived. It was not revised but instead was simply replaced by SIOP 63. However, SIOP 63 underwent four revisions, and SIOP 64 underwent eight. Table 4 below identifies the plans and revisions along with the effective dates for each. [93]

Table 4: Early SIOP Iterations and Effective Dates

SIOP Plan and Revision	Effective Dates
SIOP 62 **Base Plan**	April 1, 1961, to July 31, 1962
SIOP 63 **Base Plan**	August 1, 1962, to February 14, 1963
SIOP 63 Revision 1	February 15, 1963, to April 14, 1963
SIOP 63 Revision 2	April 15, 1963, to June 30, 1963
SIOP 63 Revision 3	July 1, 1963, to August 31, 1963
SIOP 63 Revision 4	September 1, 1963, to December, 31 1963
SIOP 64 **Base Plan**	January 1, 1964, to March 31, 1964
SIOP 64 Revision 1	April 1, 1964, to June 30, 1964
SIOP 64 Revision 2	July 1, 1964, to September 30, 1964
SIOP 64 Revision 3	October 1, 1964, to December 31, 1964
SIOP 64 Revision 4	January 1, 1965, to March 31, 1965
SIOP 64 Revision 5	April 1,1965, to June 30, 1965
SIOP 64 Revision 6	July 1, 1965, to November 9, 1965
SIOP 64 Revision 7	November 10, 1965, to March, 31 1966
SIOP 64 Revision 8	April 1, 1966, to June 30, 1966

93. Office of the Secretary of Defense, Historical Office, "History of the Strategic Arms Competition: 1945-1972," March 1981, page 597.

Together, these 15 different iterations provided the United States with an operational war plan that helped deter the Soviet Union and ensure the U.S. military was ready to fight and win a nuclear war. SAC historians note that "the most permanent thing about the SIOP was its impermanence" due to the continual iterative process.[94] Many of the iterations were driven by increases in Soviet offensive and defense forces (i.e., target growth), as well as the growth of the U.S. missile force.[95] At the end of these iterations, the U.S. possessed an operational plan for fighting a nuclear war that included second-strike capabilities, flexibility, diverse forces, city avoidance, and command and control.[96]

National Security Council Report 68

The tasking for NSC 68 came in the form of a presidential directive dated January 31, 1950, which called for "the Secretary of State and the Secretary of Defense to undertake a reexamination of our objectives in peace and war and of the effect of these objectives on our strategic plans, in the light of the probable fission bomb capability and possible thermonuclear bomb capability of the Soviet Union."[97] Like the goal of consolidation in the National Security Act of 1947, the need to reduce bureaucratic redundancies was paramount to maintaining an effective U.S. nuclear force capable of addressing the threat of a nuclear-armed Soviet Union. NSC 68 argued for a buildup of U.S. nuclear forces, among other things. At the center of the NSC 68 debate were Executive Secretary of the National Security Council James Lay Jr., Secretary of State Dean Acheson, Secretary of Defense Louis Johnson, and Paul Nitze, representing the State Department Policy Planning Staff. National Security Council officials presented NSC 68 to President Truman on April 7, 1950.

National Security Council Report 162/2

The National Security Council created NSC 162/2 to outline the basic national security policy that would be used to meet the Soviet threat while preserving U.S. economic prosperity and defensive security. NSC 162/2 outlines the strategic U.S. objectives for reducing the Soviet threat, including improving U.S. power and international position to counter the Soviet bloc; keeping the possibility of negotiation with the Soviet Union and China open; and continuing to promote capabilities among U.S. allies for preventing Soviet aggression aimed at other nations.[98] To accomplish these goals, NSC 162/2 outlined plans to maintain nuclear armaments, projecting deterrence for the U.S. and its allies,

94. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 64, Volume I Narrative," page 10. (https://archive.org/details/HistoryoftheJointStrategicPlanningStaffPreparationofSIOP64)
95. Ibid, page 12.
96. Andrew May, "The RAND Corporation and the Dynamics of American Strategic Thought, 1946-1962," Doctoral Dissertation, August 6, 1998, page 417.
97. Report to the National Security Council, "United States Objectives and Programs for National Security," April 12, 1950. (https://www.trumanlibrary.org/whistlestop/study_collections/coldwar/documents/pdf/10-1.pdf).
98. Executive Secretary of the NSC James Lay Jr., "NSC 162/2," October 30, 1953. (https://fas.org/irp/offdocs/nsc-hst/nsc-162-2.pdf)

and hindering Soviet expansionism. The contributors to NSC 162/2 were Executive Secretary of the National Security Council James Lay, Jr., National Security Planning Board Assistant Marion Boggs, State Department Director of the Policy Planning Staff Robert Bowie, Chairman of the Joint Chiefs of Staff Admiral Arthur Radford, and General of the Strategic Air Command Curtis LeMay. The executive secretary presented NSC 162/2 on October 30, 1953. This is what ultimately led to the "optimum mix" strategy that blended counterforce targeting with attacks on Soviet cities.[99]

SIOP 62

In the spirit of the Defense Reorganization Act of 1958, Secretary of Defense Thomas Gates established the Joint Strategic Target Planning Staff (JSTPS) on August 16, 1960, with the goal of bringing together conventional military elements with a strategic nuclear capability.[100] This staff was then charged with developing a SIOP to resolve lingering disputes over nuclear war planning and ensure an efficient and integrated plan should the U.S. strategic arsenal be needed. The planners debated target selection, the establishment of an intelligence advisory board, and how to build and maintain an effective nuclear force structure. The main contributors – Commander of SAC General Thomas Power; State Department Director of the Policy Planning Staff Gerard Smith; National Security Advisor McGeorge "Mac" Bundy; and Secretary of Defense Thomas Gates – created the plan in four short months. (By contrast, SIOP 63 took twice as long to develop despite starting with an existing plan in place.)[101] Approved in December 1960 and effective as of April 1 of the next year, SIOP 62 represented a continuation of the "optimum mix" strategy.[102]

SIOP 63

President Kennedy requested SIOP 63 to address some of the challenges and lessons learned from SIOP 62 and the president's dissatisfaction with his nuclear options following the Cuban Missile Crisis. The primary debate surrounding SIOP 63 was in the areas of targeting, projecting an effective deterrent, and how to arrange an effective nuclear force posture.[103] SIOP 63 also sought to add more flexibility in response options.[104] The main contributors on these issues were National Security Advisor

99. Andrew May, "The RAND Corporation and the Dynamics of American Strategic Thought, 1946-1962," Doctoral Dissertation, August 6, 1998, page 283.
100. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Background and Preparation of SIOP-62," December 14, 1960. (http://nsarchive2.gwu.edu//nukevault/ebb236/SIOP-62%20history.pdf)
101. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964, page 27. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)
102. Andrew May, "The RAND Corporation and the Dynamics of American Strategic Thought, 1946-1962," Doctoral Dissertation, August 6, 1998, page 363.
103. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)
104. However, it would not be until National Security Decision Memorandum 242 in 1974 that the use of limited nuclear options to respond to a nuclear first strike was introduced. NSDM 242 allowed the U.S. to use nuclear weapons in a retaliatory strike without escalating to an all-out nuclear exchange.

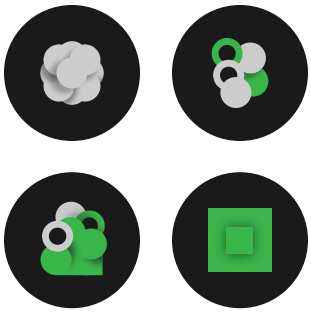
McGeorge "Mac" Bundy, General of the Strategic Air Command Thomas Power, State Department Director of the Policy Planning Staff Walt Whitman Rostow, Secretary of Defense Robert McNamara, and Commander in Chief, Pacific Fleet Admiral U.S. Grant Sharp, Jr. SIOP 63 went into effect on August 1, 1962.[105]

SIOP 64

SIOP 64 entailed changes such as the phasing out of the medium bomber force and replacement of early-model intercontinental ballistic missiles (ICBMs) with more sophisticated weapon systems with higher reliability. Additionally, major growth in overall deployed strategic delivery vehicles and deployed nuclear warheads in the U.S. nuclear arsenal necessitated that SIOP 64 be much larger and more complex than its predecessors, accounting for 4,826 operational weapons and 2,836 delivery vehicles aimed at 1,716 designated targets. The key contributors to SIOP 64 included Vice Admiral Robert Stroh, deputy director of the Joint Strategic Target Planning Staff; E. R. Caywood, director of the Strategic Air Command Historical and Research Staff; Henry David Owen, director of the State Department Policy Planning Staff; and General of the Strategic Air Command Joseph Nazzaro. SIOP 64 went into effect on January 1, 1964.[106]

105. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Preparation of SIOP 63," January 1964, page 28. (https://nsarchive2.gwu.edu/nukevault/ebb236/SIOP-63.pdf)
106. U.S. Strategic Air Command, "History of the Joint Strategic Target Planning Staff: Revisions 1-8 to SIOP 64," pages 1 & 18. (https://archive.org/details/HistoryoftheJointStrategicPlanningStaffPreparationofSIOP64)

Appendix II: Overview of Deterrence Theory and Cyber Warfare



Modern deterrence theory is largely built upon the work of theorists like Bernard Brodie, Herman Kahn, and Thomas Schelling.[107] These and other academics developed theories of deterrence to come to grips with the power and potential devastation of nuclear weapons. Deterrence theory was designed to avert a world war by helping policymakers understand the psychological framework associated with these new weapons.

Ultimately, deterrence is the manipulation of the cost/benefit calculation an adversary undertakes related to a given action. A nation can convince its adversary to avoid taking a specific action by reducing the prospective benefits and/or increasing the prospective costs. The former is called *deterrence by denial* (the power to deny military victory), and the latter is *deterrence by punishment or reprisal* (the power to hurt).[108] Cyber deterrence is therefore the similar manipulation of an adversary's cost/benefit analysis.[109] In the nuclear context, complete defense was impossible, so deterrence by punishment was the primary approach.[110] Further, nuclear deterrence sought to deter any nuclear attack (as well as other major aggressive behaviors, such as a Soviet invasion of Western Europe with conventional forces). Today, it may be impossible to deter all types of offensive cyber operations, specifically cyber crime and espionage. Rather, the target of deterrence is nation-state offensive cyber operations that cause strategic damage. Either deterrence by denial or deterrence by punishment may apply in the case of a cyber attack. However, two major challenges exist: attribution for an attack and the uncertain effects of an attack.[111]

---

107. For reasons examined in this section, it may be necessary to update Herman Kahn's six desirable characteristics of deterrence – (1) frightening; (2) inexorable; (3) persuasive; (4) cheap; (5) non-accident prone; (6) controllable – to include a seventh for cyber deterrence: Recognized.

108. In the context of deterring cyber attacks, deterrence by punishment can be through retaliatory cyber attacks (deterrence-in-kind) or other means, such as a kinetic or diplomatic response (cross-domain-deterrence).

109. Samantha Ravich and Annie Fixler, "Framework and Terminology for Understanding Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, February 22, 2017. (https://www.fdd.org/analysis/2017/02/22/framework-and-terminology-for-understanding-cyber-enabled-economic-warfare/)

110. Andrew May, "The RAND Corporation and the Dynamics of American Strategic Thought, 1946-1962," Doctoral Dissertation, August 6, 1998, page 225. This idea of the impossibility of defense began to change with President Reagan's pursuit of the Strategic Defense Initiative and improved missile defense technologies.

111. For an analysis of the other factors that complicate the application of deterrence to cyberspace, see Martin Libicki, *Cyber Deterrence and Cyber War* (Santa Monica: RAND Corporation, 2009). (https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf); Joseph Nye, "Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly*, Winter 2011. (https://dash.harvard.edu/bitstream/handle/1/8052146/Nye-NuclearLessons.pdf); Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Oxford: Oxford UP, 2017); Emily Goldman and John Arquilla, eds, *Cyber Analogies* (Monterey, CA: Naval Postgraduate School, 2014). (https://calhoun.nps.edu/bitstream/handle/10945/40037/NPS-DA-14-001.pdf?sequence=1&isAllowed=y); U.S. Department of Defense, Defense Science Board, "Task Force on Cyber Deterrence," February 2017. (http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf); Joseph Nye, "Deterrence and Dissuasion in Cyberspace," *International Security*, Winter 2016/17. (https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266)

The major problem posed by most cyber weapons is the challenge of properly attributing the attack once it has occurred. It can be difficult to conclusively determine the origin, identity, and intent of an actor/attacker operating in this domain, and defenders generally lack the tools needed to reliably trace an attack back to the actual attacker. Peter Singer and Allen Friedman have identified this lack of attribution as the key factor that prohibits the direct and immediate application of deterrence theory to the cyber realm.[112] If an attack is attributable, then traditional deterrence applies, enhanced by the possibility of a conventional military response. If an attacker believes he can get away with the operation because it is not attributable or will be falsely attributed to another actor, he may not be able to resist the appeal of using such a weapon.

Uncertainly regarding the effects of cyber weapons also significantly impacts the logic of deterrence. Defenders may have effective countermeasures to thwart cyber attacks, such as instantaneous network reconfiguration or firewalls. Similarly, routine network modification may render a cyber weapon inoperative. Available defenses, and the potential for network evolution to mitigate the effects of an attack given early warning, require cyber attackers to rely on surprise for much of their effectiveness. This situation creates instability (rather than stable deterrence) and incentivizes a first strike. Furthermore, to achieve surprise, secrecy is required, reducing the ability of a state to make credible, specific threats, because publicizing capabilities enables the threatened state to take protective actions that could blunt the impact of the revealed capability.

Cyber weapons themselves can also be unpredictable and can evolve, thus creating further uncertainty about their effects.[113] Network interdependencies also create the potential for collateral damage, with significant unintended consequences. The adverse consequences of such unintended results have been a concern for the United States. In 2003, the United States was planning, and had the capability to conduct, a massive cyber attack on Iraq in advance of the physical invasion – freezing bank accounts and crippling government systems. The Bush administration canceled the plan, however, out of a concern that the effects would not be contained to Iraq.[114] Of course, this is not say that other states would be similarly deterred from such actions.

Essentially, although cyber weapons have the potential to inflict unacceptable damage against an adversary, they are likely unable to offer states a credible, consistent, and "assured" capability for doing so. This deficiency significantly undermines their suitability as a deterrent tool. Instead, they are more likely to support an intelligence, surveillance, and reconnaissance mission, or to be used preemptively, as a first-strike weapon, or as force multipliers.

---

112. Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford UP, 2013), pages 144-148.
113. For an example, see: Kelly Burton, "The Conficker Worm," *SANS*, accessed January 2, 2019. (https://www.sans.org/security-resources/malwarefaq/conficker-worm)
114. John Markoff and Thom Shanker, "Halted '03 Plan Illustrates U.S. Fear of Cyber Risk," *The New York Times*, August 1, 2009. (http://www.nytimes.com/2009/08/02/us/politics/02cyber.html)

Acknowledgements

I would like to begin by thanking the Foundation for Defense of Democracies for launching a cyber-enabled economic warfare project and for supporting important scholarship in this field. I would like to thank Dr. Samantha Ravich for her invaluable assistance in the original conception of the idea and the framing of the research agenda and Annie Fixler for her exceptional guidance and efforts to help steer this project to completion. I would also like to thank the Digital Issues Discussion Group – particularly Nadiya Kostyuk, Chris Whyte, Brandon Valeriano, and Herb Lin – for their constructive criticism and feedback.

Cover Illustration by Daniel Ackerman

About the Author

Brian M. Mazanec, Ph.D. is a professor at Missouri State University's Department of Defense and Strategic Studies. Dr. Mazanec is also an acting director with the U.S. government with experience supporting Congress, the Office of the Secretary of Defense, the Joint Staff, Defense Threat Reduction Agency, Department of Homeland Security, and the Intelligence Community. He has been published in numerous journals, and he is the author of *The Evolution of Cyber War* (2015) and co-author of *Deterring Cyber Warfare* (2014) and *Understanding Cyber Warfare: Politics, Policy and Strategy* (2018). He received his Ph.D. from George Mason University's Schar School of Policy and Government; an M.S. in defense and strategic studies from Missouri State University's Department of Defense and Strategic Studies; and a B.A. in political science from the University of Richmond. He is an alumnus of FDD's National Security Fellows Program.

The views expressed here are solely those of the author in his private capacity and do not represent the views of any organization. Dr. Mazanec can be reached at brianmazanec@gmail.com.

About the Foundation for Defense of Democracies

The Foundation for Defense of Democracies (FDD) is a Washington, DC-based non-partisan policy institute focusing on foreign policy and national security. For more information, please visit www.fdd.org.

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

P.O. Box 33249
Washington, DC 20033-3249
(202) 207-0190
www.fdd.org