Where is the folder?

Revisiting NSC 68: Crafting a Modern Intelligence Directive

28JUL2024
Peter Skrzypczak

Summary of Significant Objectives and Rationale

The landmark National Security Council document NSC 68, titled "United States Objectives and Programs for National Security," laid out a comprehensive strategy for containing Soviet expansion and bolstering American power during the early Cold War era (Kaura, 2020). At its core, the directive recognized the ideological and geopolitical struggle between the United States and the Soviet Union, and the urgent need to strengthen U.S. military capabilities, economic might, and global influence to counter the communist threat (Johnson, 1988).

The document identified several key objectives, including maintaining military superiority, promoting economic prosperity, and shoring up alliances worldwide (Marklund et al., 2010). Crucially, it emphasized the importance of a whole-of-government approach, drawing on diplomatic, informational, military, and economic instruments of national power to achieve strategic aims (Marklund et al., 2010). Perhaps most significantly, NSC 68 marked a shift from the more passive, reactive posture of earlier containment policies, toward a more proactive, globe-spanning effort to roll back Soviet influence and cement American global leadership (Johnson, 1988).

What Would A Derivative Actionable Intelligence Directive Look Like in Current Times?

Based on the principles and priorities outlined in NSC 68, a modern intelligence directive might include the following elements:

Intelligence Objectives:

Closely monitor and assess the military capabilities, strategic ambitions, and malign activities of nation-state competitors, such as China and Russia, that seek to challenge U.S. global influence, undermine the rules-based international order, and erode America's technological edge. (Vencel et al., 2018) (Riste, 2009)

Develop comprehensive threat assessments and early warning indicators to anticipate and preempt adversary aggression, cyberattacks, and other forms of asymmetric warfare. (Maughan, 2010) (Dolman, 2000)

Enhance cooperation with allies and partners to share intelligence, coordinate response strategies, and bolster collective security. (Gilad et al., 2020)

Intelligence Collection and Analysis:

Leverage a diverse array of human, signals, and geospatial intelligence sources to gather detailed, real-time information on adversary intentions and capabilities. (Gilad et al., 2020) (Dolman, 2000)

Invest in advanced data analytics, artificial intelligence, and other emerging technologies to rapidly process and interpret intelligence, identify patterns, and generate actionable insights. (Maughan, 2010)

Strengthen coordination and information-sharing between the intelligence community, law enforcement, and other national security stakeholders to enable a whole-of-government approach. (Gilad et al., 2020) (Dolman, 2000)

Intelligence Dissemination and Utilization:

Ensure timely, tailored, and user-friendly intelligence products reach key decision-makers, military commanders, and other relevant consumers to inform policymaking, operational planning, and strategic decision-making. (MacArtney, 1988)

Leverage intelligence to drive proactive and anticipatory actions, rather than solely reactive responses, to stay ahead of evolving threats. (Maughan, 2010) (Gilad et al., 2020)

Questions for Further Consideration

How can the intelligence community better adapt to the dynamic, fast-paced, and technologically complex security environment of the 21st century?

What steps should be taken to enhance coordination, integration, and interoperability between the various components of the U.S. intelligence apparatus?

How can the United States leverage intelligence to bolster its economic competitiveness and technological edge in the face of strategic competition from China and other rivals? (Degaut, 2015)

Comparative Critique

While the core objectives and strategic rationale outlined in NSC 68 remain highly relevant, the contemporary security landscape has evolved dramatically since the document's formulation in 1950. The rise of cyberspace as a critical domain of conflict, the proliferation of non-state and asymmetric threats, and the intensification of great power competition have all necessitated significant adaptations in the way the United States approaches intelligence and national security.

Notably, the intelligence community has had to grapple with the challenges posed by the "information revolution," including the exponential growth of open-source data, the increasing use of social media and other digital platforms by adversaries, and the need to develop new analytical tools and tradecraft to effectively process and leverage this deluge of information. (Degaut, 2015) (Bury & Chertoff, 2020)

Additionally, the evolving nature of warfare, with its blurring of the lines between peacetime and conflict, has required a more proactive, anticipatory intelligence posture that can identify and disrupt threats before they materialize. This shift has placed a greater premium on strategic foresight, early warning, and the ability to rapidly adapt to rapidly changing circumstances. (Dolman, 2000)

A Sample Memo Outlining an Actionable Intelligence Directive Designed for Current Times?

“In light of the evolving geopolitical landscape and emerging security challenges, the National Security Council hereby directs the Intelligence Community to undertake the following actions:

Continuously monitor and assess the capabilities, intentions, and activities of near-peer adversaries and other state actors that pose a threat to U.S. national security interests. Leverage advanced data analytics, artificial intelligence, and other emerging technologies to enhance early warning and anticipate potential flashpoints or destabilizing events (Maughan, 2010) (Vencel et al., 2018).

Strengthen intelligence-sharing and collaboration with key allies and partners, both bilaterally and through multilateral frameworks, to build a comprehensive understanding of global threats and devise coordinated responses (Dolman, 2000). Elevate cybersecurity as a top priority, working closely with the private sector to defend critical infrastructure and information systems against malicious cyber actors (Maughan, 2010).

Develop tailored influence and information operations campaigns to counter adversary propaganda, expose their misdeeds, and bolster the legitimacy and soft power of the United States and its allies. Leverage media, social platforms, and other communications channels to shape the global narrative and offer a compelling alternative to authoritarian models (White House Report: National Security Strategy for a New Century, 1997).”

Policy Improvement Questions

To enhance the overall effectiveness of national security policy in the current strategic environment, the following questions merit careful consideration:

What new geopolitical and technological trends, such as the rise of China, the proliferation of disruptive technologies, and the weaponization of information, should be factored into the design and implementation of national security strategy?

How can the Intelligence Community better anticipate and respond to unconventional, asymmetric threats, such as insurgencies, cyber attacks, and the exploitation of social divisions, that challenge traditional military superiority?

What institutional reforms or organizational changes are needed to foster greater agility, collaboration, and integration within the Intelligence Community and between intelligence, policymakers, and other key stakeholders? (Bury & Chertoff, 2020)

Comparative Critique

The core objectives and strategic rationale outlined in NSC 68 remain relevant in the contemporary security landscape, as the United States continues to confront determined adversaries seeking to erode American power and influence. However, the evolving nature of threats, the proliferation of disruptive technologies, and the increasingly complex geopolitical environment necessitate a fresh approach that builds upon the foundational principles of NSC 68 (Thal & Heuck, 2010).

Critically, the directive must adapt to the realities of a multipolar world, where the challenge from China has emerged as a central concern, and the global information environment has become a new battleground (Efthymiopoulos, 2019). Furthermore, the growing salience of non-traditional security threats, such as cyber attacks, disinformation campaigns, and the exploitation of societal fissures, demands a more comprehensive and integrated response that leverages the full spectrum of national power (Pierce et al., 2022).

By incorporating these elements and empowering the Intelligence Community to spearhead innovative, proactive measures, the updated directive can help strengthen the United States' strategic posture, bolster its global influence, and safeguard its vital interests in the decades to come (Schoka, 2019).

In Conclusion

In conclusion, the United States must continue to adapt its intelligence and national security apparatus to address the evolving challenges of the 21st century. By harnessing emerging technologies, deepening international cooperation, and developing tailored influence operations, the Intelligence Community can help the nation maintain its strategic edge and protect its vital interests in an increasingly complex and contested global environment. As the United States navigates this new era of strategic competition, the lessons of NSC 68 remain instructive, but must be continually refined and reinvigorated to meet the demands of the modern security landscape.

References:

Kaura, V. (2020, November 9). India's National Security Coordination and Policymaking. Routledge, 165(7), 68-84. https://doi.org/10.1080/03071847.2021.1896378

Johnson, R H. (1988, January 1). Misguided Morality: Ethics and the Reagan Doctrine. Oxford University Press, 103(3), 509-529. https://doi.org/10.2307/2150761

Marklund, L A., Graham, A., Morton, P G., Hurst, C G., Motola, I., Robinson, D W., Kelley, V A., Elenberg, K., Russler, M F., Boehm, D E., Higgins, D M., McAndrew, P., Williamson, H M., Atwood, R D., Huebner, K., Brotons, A A., Miller, G T., Rimpel, L Y., Harris, L L., . . . Cantrell, L. (2010, October 1). Collaboration between Civilian and Military Healthcare Professionals: A Better Way for Planning, Preparing, and Responding to All Hazard Domestic Events. Cambridge University Press, 25(5), 399-412. https://doi.org/10.1017/s1049023x00008451

Vencel, L., Sweetman, E., & Lante, N. (2018, July 1). Composing Complex Capability: The Stakeholder Driven Development Framework. Wiley, 28(1), 1519-1533. https://doi.org/10.1002/j.2334-5837.2018.00565.x

Riste, O. (2009, June 22). The Intelligence–Policy Maker Relationship and the Politicization of Intelligence. Cambridge University Press, 179-209. https://doi.org/10.1017/cbo9781139174541.009

Maughan, D. (2010, February 1). The need for a national cybersecurity research and development agenda. Association for Computing Machinery, 53(2), 29-31. https://doi.org/10.1145/1646353.1646365

Dolman, E C. (2000, January 1). Military intelligence and the problem of legitimacy: Opening the model. Routledge, 11(1), 26-43. https://doi.org/10.1080/09592310008423259

Gilad, A., Pecht, E., & Tishler, A. (2020, July 18). Intelligence, Cyberspace, and National Security. Taylor & Francis, 32(1), 18-45. https://doi.org/10.1080/10242694.2020.1778966

MacArtney, J. (1988, December 1). Intelligence: A consumer's guide*. Taylor & Francis, 2(4), 457-486. https://doi.org/10.1080/08850608808435077

Degaut, M. (2015, March 19). Spies and Policymakers: Intelligence in the Information Age. Taylor & Francis, 31(4), 509-531. https://doi.org/10.1080/02684527.2015.1017931

Bury, P., & Chertoff, M. (2020, June 6). New Intelligence Strategies for a New Decade. Routledge, 165(4), 42-53. https://doi.org/10.1080/03071847.2020.1802945

White House Report: National Security Strategy for a New Century. (1997, August 1). Cambridge University Press, 8(4), 29-49. https://doi.org/10.1017/s105270360000174x

Thal, A E., & Heuck, W D. (2010, April 13). Military technology development: a future-based approach using scenarios. Emerald Publishing Limited, 12(2), 49-65. https://doi.org/10.1108/14636681011035744

Efthymiopoulos, M P. (2019, June 24). A cyber-security framework for development, defense and innovation at NATO. Springer Nature, 8(1). https://doi.org/10.1186/s13731-019-0105-z

Pierce, G L., Holland, C., Cleary, P F., & Rabrenovic, G. (2022, October 28). The opportunity costs of the politics of division and disinformation in the context of the twenty-first century security deficit. Springer Nature, 2(11). https://doi.org/10.1007/s43545-022-00514-5

Schoka, A J. (2019, October 1). Prioritizing Strategic Cyberspace Lethality. National Numeracy Network, 4(1). https://doi.org/10.5038/2378-0789.4.1.1049