Security Watch: No-Fly Zones and Flying Blind

Editor

Follow this and additional works at: https://commons.erau.edu/ibpp

Part of the Aviation Safety and Security Commons, Defense and Security Studies Commons, International Relations Commons, Other Political Science Commons, Other Psychology Commons, Peace and Conflict Studies Commons, and the Terrorism Studies Commons

Recommended Citation


This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in International Bulletin of Political Psychology by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu, wolfe309@erau.edu.
Title: Security Watch: No-Fly Zones and Flying Blind
Author: Editor
Volume: 14
Issue: 16
Date: 2003-05-22
Keywords: Air Space, Aviation, Homeland Security, Security

Abstract: The article evaluates the gain in security from no-fly zones from a security perspective.

In the context of homeland security within the United States, one might ask how much security is obtained from establishing and maintaining a public policy of a no-fly zone—i.e., proscribing an air space defined by area and elevation for aircraft operations. In seeking an answer or answers to this question, one can take the perspectives of vulnerability, threat, or the integration of the two.

From a vulnerability perspective, one would look at systematically and unsystematically obtained empirical data, employ the inferred mental processes of reason and logic, consult expert opinion, and/or employ beliefs that are believed to be true just because they are believed to be true about what could happen at a specific location. For example, one could speculate or even develop realistic simulations that a specific catastrophic event could occur for a specific combination of characteristics. Of special note might be aircraft characteristics including weight, payload, and speed; atmospheric characteristics such as ambient temperature, humidity, and wind; and ground characteristics such as topology, population, building structures, and so-called dangerous substances—the last including just about anything depending on circumstances. Based on cognitive and political heuristics bearing on the assumed frequency and/or severity of specific catastrophic events, security authorities would construct a no-fly zone to address some especially egregious, hypothesized event or combination thereof.

From a threat perspective, one would look at intelligence bearing on the probabilities that individuals, groups, organizations, governments, and other political actors may attack a specific, physical location at least partially through use of an aircraft. The intelligence would be collected and analyzed within the same epistemological constraints as above: viz., empiricism, reason and logic, expert opinion, and beliefs that are believed because they are believed. Again, there would be cognitive and political heuristics applied in developing probabilities and in estimating frequency and severity of specific catastrophic events. The result may be the construction of a no-fly zone.

From a perspective of vulnerability-threat integration, one would look at both vulnerability and threat. In the abstract, both huge vulnerability but no threat and the converse of no vulnerability but huge threat might suggest no need for action. However, in the real world, the states of no vulnerability and of no threat may not exist. So, it is the matching of specific degrees of assumed vulnerability and threat within a political environment that would dictate a go/no-go decision concerning a no-fly zone. Here the political environment would comprise the fact of finite security resources, the opinion of segments of the general public, and various assumptions about success and failure in the roles of a political leader and a security professional.

Through a peremptory analysis of public discourse among political leaders and security professionals, one can identify all three perspectives. Vulnerability perspectives are often intrinsic to some corporate entities attempting to sell security products (often ingenious and technologically breath-taking) in a hot security market. A related aphorism for some of these entities might be that where there’s a vulnerability, there’s an opportunity for profit.
Threat perspectives have long been within the domain of intelligence professionals. However, these professionals always will continue to wrestle with obtaining the best combination of analyzed technical intelligence, accurate and relevant human intelligence, and a responsive and securely transmitted final product to security professionals.