



## Editor's picks

### China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities; Countering Insurgency and the Myth of "The Cause;" Engaging Non-state Security Providers: Whither the Rule of Law?; Irrational Rationality of Terrorism; and Operationalizing Protection of Civilians in NATO Operations

It is possible for an insurgency to develop from a single cause, for the insurgents to identify and communicate this unifying cause to the population, and for the insurgents to remain steadfastly focused even as counterinsurgents undermine their organization and redress the cause, posit Dr. Daniel Cox and Dr. Alex Ryan in *Countering Insurgency and the Myth of "The Cause."* But often the case is that there is no *single* cause, rather that popular support is mobilized by appealing to multiple motivations, and that by the time counterinsurgents resolve the initial grievance, the insurgency has found alternative justifications to mobilize popular support. Since insurgent leadership is often competent and adaptive, it would be wise to consider the latter scenario against any counterinsurgency strategy. Yet, even when this is acknowledged in the counterinsurgency literature, the theory is remarkably silent how this affects the choice of operational approach. Cox and Ryan address this gap and offer a framework for more accurately mapping, understanding, anticipating, and addressing the multiple causes that draw adherents to insurgency and allow for its perpetuation.

Dr. Robert Nalbandov deals with the ontological problem of applying the rational choice frameworks to the study of terrorism in *Irrational Rationality of Terrorism*. He tests the application of the rational choice to "old" (before the end of the Cold War) and "new" (after the end of the Cold War) iterations of terrorism. He starts with analyzing the fundamentals of rationality and applies it at two levels—the individual (actors) and group (collective)—via two outlooks: tactical (short-term) and strategic (long-term). The main argument of the article is that, while old iterations of terrorism can be explai-

ned by the rational choice theory, new iterations of terrorism represent a substantial departure from rationality.

The primacy of the rule of law has long been seen as one of the essential principles of security sector reform (SSR) programming, and part of the larger gospel of SSR is that the accountability of security providers is best guaranteed by embedding security governance within a rule of law framework. In *Engaging Non-state Security Providers: Whither the Rule of Law?*, Dr. Timothy Donais argues that acknowledging the reality of nonstate security provision, however, presents a challenge to thinking about SSR as merely the extension of the rule of law into the security realm—in large part because whatever legitimacy nonstate security providers possess tends to be grounded in *extralegal* foundations. This paper—more conceptual than empirical in its approach—considers the implications of hybrid forms of security governance for thinking about the relationship between SSR and rule of law promotion and argues that the rule of law still provides a useful source of strategic direction for SSR programming.

In *China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities*, Mr. Emilio Iasiello affirms that China is engaged in longstanding cyber espionage against the United States, as well as other nations, to collect sensitive public and private information in support of national objectives laid out in its 12th Five-Year Plan. Foreign governments, citing China's malfeasance, have rebuked these activities—a claim vehemently denied by Beijing. In response, China is leveraging the *Three Warfares*, an integrated three-prong information warfare strategy, to combat these accusations by leveraging media, legal, and psychological components designed to influence the international community. While the United States has threatened the imposition of economic sanctions, Beijing has successfully parried consequential actions by arresting US-identified hackers, thereby demonstrating the regime's commitment toward preserving a stable and peaceful cyberspace. These interrelated *Three Warfares* disciplines have targeted the cognitive processes of the US leadership, as well as the international public's perception of China as a global threat, thereby successfully forestalling the implementation of any effective punitive or economic deterrence strategy, including the imposition of cyber sanctions.

In *Operationalizing Protection of Civilians in NATO Operations*, Ms. Marla Keenan and Mr. Alexander Beadle contend that though NATO and other military forces increasingly recognize protection of civilians as a key objective in their operations, implementation remains challenging. To effectively provide such protection, the military force must understand the threats that exist and match capabilities to counter those threats. The authors strongly believe that military planners need a more formal structure to conceptualize physical protection, and herein outline “The Protection Ladder” as a tool for military planners and leaders to explain the legal obligations and additional

operational capabilities necessary for civilian protection. The article offers practical suggestions on how civilian protection can be effectively addressed before, during, and after military operations. NATO should develop its protection capabilities, because future mission success depends upon it.

Rémy M. Mauduit, Editor  
*Air & Space Power Journal–Africa and Francophonie*  
Maxwell AFB, Alabama