

Book Review: International Security: The Contemporary Agenda

Blog Admin

What are the the key security challenges and developments in the post–Cold War world? Drawing on a wide range of contemporary examples from the Iraq war to the rise of China, **Roland Dannreuther** aims to guide readers through cyber attacks, environmental security, and drone warfare. **Kai Chen** finds that this is a thought provoking look at both current and future thinking in security and IR.

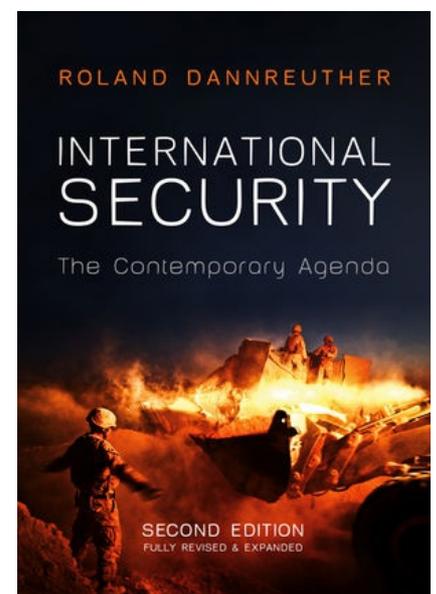


International Security: The Contemporary Agenda. Second Edition. Roland Dannreuther. Polity Press. May 2013.

Find this book:

[Roland Dannreuther](#)'s expanded second edition of *International Security: The Contemporary Agenda* aims to analyse the key security challenges and developments in the post–Cold War world and rethink the long-lasting debates among the realist, constructionist and neo-realist schools of thought in international security. Dannreuther's main aim is to provide an insightful overview of the most critical security threats, which "have direct meaning for our everyday existence and for international politics more generally" (p.3). The author, currently head of the department of Politics and International Relations at the University of Westminster, has published on these topics many times before, and with this book he aims to engage students and policy makers.

Dannreuther focuses upon the most challenging of international security issues, such as environmental security, migration, terrorism, proliferation of weapons of mass destruction and so on. The book is divided into four parts. Part 1 (chapter 1-2) overviews post-Cold War rethinking of international security, and Part 2 (chapter 3-5) includes a comparative analysis on collective security cooperation in Europe and Asia. In Part 3 (chapter 6-8), Dannreuther focuses on the debates on environmental security (e.g. conflicts for oil and water), and also explains the critical security threats presented by migration. Part 4 (chapter 9-11) discusses the dynamics of the asymmetric security challenges in the world, including international terrorism and cyber-warfare. It is worth noting that chapter 11 is written by Jamie Allinson, who also provides contributions in updating the section on critical security studies in chapter 2. In my view, the most attractive chapters are the newly added ones (chapters 5 and 11), which clearly show the tensions between theory and practice in international security.



kindle edition

amazon

Can alliances and collective security be mutually inclusive? In Chapter 5, “Collective Security, Alliances and Security Cooperation”, Dannreuther analyses the multiple interlocking security institutions in Europe and Asia. In the analysis of Europe, this chapter mainly focuses on NATO, and highlights that NATO “does present a marriage of collective defence and collective security capacities” (p.125). By contrast, there is only “complex blending of alliance and a nascent security community” (p.114) in Asian security institutions (e.g. ASEAN and Shanghai Cooperation Organization). This distinction exists due to the different historical, social-economic and cultural contexts in Europe and Asia, writes Dannreuther. For example, a cohesive security community has emerged in Europe, because multilateral cooperations (e.g. economic, political and military) have been established for a long time. In contrast, “territorial disputes, ideological confrontations, and traditional enmities between the states” remain “salient features” (p.126) in Asia. As a result, NATO is more developmental and prioritises collective security functions, but in Asia long-lasting territorial and ideological tensions mean “there is a complex balance of power which underpins the regional security order” in Asia (p.130). Though ASEAN and Shanghai Cooperation Organization seek to promote security cooperations, they both have their own weak points. For instance, ASEAN, which aims at constructing institutionalized security cooperation, is “an intrinsically weak organization” to coordinate the great powers of the region (e.g. China, Russia or the United States). In addition, the ability of Shanghai Cooperation Organization—a collective security institution meeting non-traditional security threats in Central Asia—is also questionable for excluding the United States.

For this reviewer, Dannreuther’s argument hits the mark. Child soldiering in Asia might also hint that the Asian security institutions still lack collective security functions to some extent. As the worst-hit region of child soldiering in the world, there are ten thousands of child soldiers across Myanmar, Thailand, Indonesia and Afghanistan. Today, Myanmar is believed to have more child soldiers than any other country in the world – over 70,000 according to a [Human Rights Watch report in 2002](#) (readers might also find statistics and case studies from [Child Soldiers International](#) of interest). However, this critical security issue is still not on the agendas of the ASEAN Regional Forum and the Shanghai Cooperation Organization.

Another critical security issue is cyber-warfare in the context of revolution of military affairs. In Chapter 11, “Cyber-Warfare and New Spaces of Security” written by Jamie Allinson, the impact of the evolution of technology on military affairs and international security is discussed. Cyber-warfare is a double-edged sword: when cyber-attacks are launched by a state, that state is of course also made vulnerable to this new security threat. At present, some major powers have prioritized cyber-warfare in their security agenda. For instance, in October 2010, [United States Cyber Command](#) reached full operational capability. Therefore, “the idea of cyber-space as an additional realm of conflict has become commonplace in the US military” (p.263). However, due to “the cheapness and universality of the technology required for an attack” (p.263), there will be more non-state actors (e.g. terrorism organisations) obtaining the abilities of conducting cyber attacks. Political hacker groups such as Anonymous have used denial of service attacks against states (p.264); even well-known hacker groups such as WikiLeaks have also been targets of cyber attacks.

However, Allinson argues that cyber-warfare will be “more of a tactical than a strategic innovation” (p.270). In my view, this argument seems to underplay the possibility that cyber-warfare would be a new domain of military strategy in the early 21st century, which will even change the perspectives of interstate and intrastate conflicts in the future. This chapter seems to ignore the involvements of private military security companies (PMSCs). Actually, PMSCs have abilities in producing drones or defending cyber attacks. Recently, a Japanese security firm named “Secom” planned to market private security drones. If PMSCs are put into the discussions of cyber-warfare, we will discover that more PMSCs are participating in this field ever before. Their employers are not limited to major powers, but include many INGOs and transnational corporations. For instance, NATO has been working with some of the world’s biggest private cyber security companies to share knowledge and experience, in order to help deter and resist cyber-attacks. In the foreseeable future, PMSCs will definitely play an essential role in cyber-warfare.

I look forward to the publication of the third edition of this well-researched book, which will hopefully explore new critical security issues in the future. In short, *International Security* is not only a thought-provoking textbook for students in the area of international security, but also a timely and insightful read for policy-makers, academics and practitioners of international relations.

Kai Chen is a post-doctoral research fellow of the Centre for Non-Traditional Security and Peaceful Development Studies, College of Public Administration, Zhejiang University, China. His research interests include geo-strategic relationship and international security in Indo-China peninsula and China. [Read more reviews by Kai Chen.](#)

