Book Review
By
AFEERA FIRDOUS

Ben Buchanan, *The Cybersecurity Dilemma-Hacking, Trust and Fear Between Nations* (London: C. Hurst & Co. (Publishers) Ltd., 2016) 289.

Ben Buchanan is a Postdoctoral Fellow at Harvard University's Belfer Center for Science and International Affairs. He specializes in relations between cybersecurity and statecraft. Ben has taken the traditional concept of security dilemma and has given a detailed account of its application to inter-state relations in the realm of cyberspace. The book, *The Cybersecurity Dilemma-Hacking, Trust and Fear Between Nations*, has eight chapters. Each chapter deals with a particular aspect of author's thesis on the subject, and a conclusion which sums up the discussions in the book. Chapter one explains the Realist approach of international relations; anarchy, absolute power, and security. These concepts originated in ancient Greece, and explain the concepts of threat, misperception and misinterpretation; and how they lead to security dilemma. This chapter also discusses the application of a traditional concept (security dilemma) in a new domain (cyberspace) and sets the tone for discussion in the subsequent chapters. The author refers to Michael Herman, a British signals officer and scholar, who for the first time applied the concept of security dilemma beyond development and deployment of military capabilities. Ben further expanded Herman's idea and applied it to foreign intelligence cyber operations. Chapter two and three explore the operational processes of network intrusion and defense. The author has named these 'Intrusion Model' and 'Network Defense Model'. He raises the question regarding the broad effects of states intruding into the networks of other states not just to enhance offensive competences but also to build their own defenses. The author goes on to distinguish between the offensive and defensive goals which can motivate a state to intrusions. While discussing potential defensive and offensive network intrusions and many risks attached to them, he states that the main theme of the book as:

> To assure their own cybersecurity, states will sometime intrude into the strategically important networks of other states and will threaten – often unintentionally – the security of those other states, risking escalation and undermining stability.

Chapter four argues how network intrusion can threaten other states and create fear among them, leading them to misperception or misinterpretation of the intent and change the conditions of conflict. Ben differentiates between two types of network intrusions; cyber exploitation and cyber-attacks; and explains their effects on the outlook of states' policies in different ways. Chapter five examines the variables of the security dilemma by applying classic mitigator logic on cyberspace and concludes that cybersecurity dilemma remains a challenge to conflict mitigation. Chapter six elucidates the importance of status quo and information distribution. The author, in this context, states that inequity in information distribution raises the severity of cybersecurity dilemma. This chapter also discusses the application of international law in cyberspace but the author has overlooked the fact that obedience of international law by states is not obligatory but voluntary. A discussion on this important factor would have added value to the examination of the subject. Chapter seven details the limitations, and objections and the future of cybersecurity dilemma. The author identifies three objections; first, difficulty of attribution of the offence; second, no network intrusion reaches the level of existential threat; and third, cyber capabilities are unevenly distributed. The chapter concludes that cybersecurity dilemma is likely to grow more compelling in coming days. Ben states that cyber threat is not an existential threat for the states, he, however, has failed to answer the question if an intruder state gets access to other state's strategic and critical national infrastructure including launching codes of nuclear weapons through intrusion or attack then what kind of response could be expected? In chapter eight, Ben argues that advancing of bilateral trust between states can avoid cybersecurity dilemma, but in realist world, achieving bilateral trust in international relations is nearly impossible; for instance, NSA's leaked documents have shown that US has spied upon the e-mails of its close allies' leadership; the German Chancellor and the Mexican President.

While concluding, the author charts out five dangers in which cybersecurity dilemma can cause substantial damage. First, cybersecurity has the potential to enhance tension and conflict not just in an actual situation but also in anticipation of a crisis, which means an insecure state is more likely to adopt offensive posture for deterrence. Second, threat prompts insecurity and tends to escalate tension. Third, the misinterpretation of intruder's intention can increase the cybersecurity dilemma. Fourth, the potential danger is that two pressures - the immediate need for bettering offensive capability and the need for better defensive security and resilience – force states into conflicting situations. Fifth, the cybersecurity dilemma can entice policy makers into potentially damaging duplicity. The fundamental basis of cybersecurity dilemma like traditional understanding of the concept is fear and escalation dynamics: fear that causes the dilemma and escalation that the dilemma brings about.

One major criticism on the book is that the discussion revolves around only one actor: the state, although non-state actors are increasingly becoming important players in network intrusions. The author also suggests deterrence and mitigation efforts as a partial way out of the problem, but doesn't explain how deterrence will work in cybersecurity domain if the intruder or attacker happens to be a non-state actor, who is irrational and has little stake in keeping peace and stability within a state, regionally or beyond?

Secondly, the author’s account of defensive intrusion and unintentional risks to other states’ security raise compelling question regarding the criteria against which a state’s intrusion may be regarded defensive in nature, while the author, himself, admits that it is a difficult task to discriminate between defensive and offensive network intrusion. The author also terms defensive-minded network intrusion as intelligence efforts, not invasions, which is a critically weak argument.

The study is drawn on the leaked documents of Edward Snowden, former NSA contractor; case studies of cyber operations in few previous years, and interviews from former officials and policy makers. The book maintains that international relations and policy are germane to cyber world as they are to the physical.

The book is a good read for international relations scholars with a non-technical background. It gives an inclusive understanding of cyber operations and how different kinds of cyber intrusions work.

Afeera Firdous is a
Research Assistant at CISS