Analysis of threat perceptions

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Analysis of threat perceptions : NATO and Türkiye's cyber terrorism policies / Mehmet Emin Erendor

Auteur(s) : Erendor, Mehmet Emin (19..-....)

Publication : Boca Raton (Fla.) [etc.] : CRC press, 2025

Description matérielle : 1 volume (XI-190 pages) ; 24 cm

Collection : Security, audit and leadership series

ISBN : 978-1-0328-0228-2
1-03-280228-6
978-1-0328-0442-2
1-03-280442-4

EAN : 9781032802282 relié
9781032804422 broché

Appartient à la collection : Security, audit and leadership series

Classification décimale Dewey : 364.168 2

Note sur les bibliographies et les index : Bibliographie pages 165-190

Note sur le contenu : Case study of cyber terrorism : Estonia The historical background of the concept of threat and the assessment of the risk Game theory The cybersecurity policy of NATO The cybersecurity policy of Türki?ye

Note de thèses et écrits académiques : Texte remanié de Doctoral thesis International relations University of Southampton (GB) 2017 An analysis of threat perceptions : combating cyber terrorism : the policies of NATO and Turkey, evaluated using game theory in the context of international law

Résumé ou extrait : "In 2007 Estonia faced a series of cyber-attacks on its cyber infrastructure, which caused widespread damage to the country's economy, politics and security. However, despite this series of cyber-attacks, NATO did not apply Article 5 of the North Atlantic Treaty due to lack of consensus on

applying Article 5 in the Estonian case. Although various approaches have been developed by scholars, there is no common application of international law in the United Nations Charter regarding cyber threats or attacks. Moreover, whilst there has been no common definition of 'cyber terrorism' by the international community, some scholars regard 'cyber-attacks' as acts of war. There is a paucity of literature dealing with the application of international law on cyber threats. A new Strategic Concept was adopted in 2010. Its most important development was to identify the significance of cyber threats to all NATO body members. When updating its own technology, the organization needs to be ready to defend itself against all kinds of asymmetrical warfare, whether from within or beyond its operational range. However, the terms of Article 5 of the North Atlantic Treaty were imprecise as to whether cyber-attacks can be regarded as a form of threat; for this reason, NATO accepted the case-by-case concept on cyber threats/attacks in terms of the application of Article 5 by the Wales Summit in 2014. Despite the fact that the Charter of the United Nations has not been revised, if its articles are broadly evaluated, cyber attacks would be accepted as a threat or use of force against the territorial integrity of a state. The main purpose of this book is to analyze and evaluate what has been carried out regarding NATO's operational arrangements and its Cyber Defense approach, and, secondly, to explain this in the lens of Game Theory. Furthermore, it will demonstrate why the web is paramount to NATO's system-driven operations, and why it requires a Cyber Defense arrangement. In particular, the research endeavors to analyze Türkiye in this regard. The cyber-attack on Estonia in 2007 will be used by way of a case study to explain the development of threat perceptions, risks, international law, cyber security policies and application of Game Theory." (page d'avant-titre)

Sujet - Collectivité : Organisation du traité de l'Atlantique nord

Sujet - Nom commun : Cyberterrorisme -- Europe
Systèmes informatiques -- Mesures de sûreté -- Évaluation du risque -- Europe
Cyberterrorisme -- Amérique du Nord
Systèmes informatiques -- Mesures de sûreté -- Évaluation du risque -- Amérique du Nord
Cyberterrorisme -- Turquie
Systèmes informatiques -- Mesures de sûreté -- Évaluation du risque -- Turquie
Politique et gouvernement -- Turquie
Théorie des jeux