A Nato Cooperative Cyber Defence Centre Of Excellence Initiative

The NATO CCD COE series of reports on national organisational models for ensuring cyber security summarise national cyber security strategy objectives and outline the division of cyber security tasks and responsibilities between agencies. In particular, the reports give an overview of the mandate, tasks and competences of the relevant organisations and the coordination between them. The scope of the reports encompasses the mandates of political and strategic cyber security governance; national cyber incident management coordination; military cyber defence; and cyber aspects of crisis prevention and crisis management.

In order to establish a comprehensive understanding of China’s cyber attitude, it is of paramount importance to know its strengths and weaknesses. For that purpose, this paper aims to give readers a detailed overview of China’s cyber capabilities, related documents and strategies, and the general command structure of its tactical execution layer. Importantly, the country’s distinct approach raises the necessity of introducing the general national strategic thinking and framework into which cyber falls. The paper acts as a comprehensive starting point for anyone aiming to get a foothold on affairs related to China and cyber.

Seventy percent of our planet is covered by water, and even in today's world of instant communication the global community is still heavily reliant on sea-based transport. The maritime domain has always been one of NATO's key strengths, but concerns about maritime security have taken on renewed importance in recent years, and NATO has been forced to re-examine some of its fundamental assumptions about the post Cold War security environment. This book shares some of the research, debates and findings from a NATO Advanced Research Workshop (ARW); Building Trust to Enhance Maritime Security, held in Geneva, Switzerland, in November 2014. The chapters in the book deal extensively with lessons learned by NATO from a wide range of policies, operations and situations. This maritime experience has been amassed from the Atlantic and Mediterranean to the Baltic and the Black Sea, and even into the Indian Ocean, as well as from the four decades spent defending NATO allies on the high seas during the Cold War. The single most profound lesson learned over the years has concerned the importance of efficient coordination. Structures and mechanisms have been created, not least in recent counter piracy operations, which enable a vast array of actors to work together in an efficient way, and which could prove invaluable in future efforts to counter terrorism and aggression worldwide. The safety of the maritime domain is essential to the freedom and security of all nations, and this book will be of interest to all those whose work involves maintaining that freedom and security.

The study outlines the division of cyber security tasks and responsibilities between different agencies, describes their mandate, tasks and competence, as well as coordination among them. In particular, it describes the mandates of political and strategic management; operational cyber security capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and crisis management. It also offers a summary of the national information society setting and e-government initiatives as well as the national cyber security strategy objectives in order to clarify the context for the organisational approach in a particular nation.

A comprehensive analysis of the international law applicable to cyber operations, including a systematic study of attribution, lawfulness and remedies.

National Cyber Security Organisation, United Kingdom
National Cyber Security Organisation, Slovakia
Excessive Maritime Claims
National Cyber Security Organisation, Israel
Understanding Cyber Conflict
L'esprit des langues françaises et italienne ou Dictionnaire abrégé de l'académie de la Crusca
National Cyber Security Organisation, France
Legal, Policy & Industry Perspectives
China and Cyber
National Cyber Security Organisation, Estonia

The 4th edition of Excessive Maritime Claims updates material on state practice of the law of the sea since publication of the 3rd edition in 2012 and adds new material on islands and other maritime features.

The Tallinn Manual on the International Law Applicable to Cyber Warfare, written at the invitation of the Centre by an independent International Group of Experts, is the result of a three-year effort to examine how extant international law norms apply to this new form of warfare. The Tallinn Manual pays particular attention to the jus ad bellum, the international law governing the resort to force by States as an instrument of their national policy, and the jus in bello, the international law regulating the conduct of armed conflict (also labelled the law of war, the law of armed conflict, or international humanitarian law). Related bodies of international law, such as the law of State responsibility and the law of the sea, are dealt within the context of these topics. The Tallinn Manual is not an official document, but instead an expression of opinions of a group of independent experts acting solely in their personal capacity. It does not represent the views of the Centre, our Sponsoring Nations, or NATO. It is also not meant to reflect NATO doctrine. Nor does it reflect the position of any organization or State represented by observers.

The cyber security of vital infrastructure and services has become a major concern for countries worldwide. The members of NATO are no exception, and they share a responsibility to help the global community to strengthen its cyber defenses against malicious cyber activity. This book presents 10 papers and 21 specific findings from the NATO Advanced Research Workshop (ARW) ‘Best Practices in Computer Network Defense (CND): Incident Detection and Response, held in Geneva, Switzerland, in September 2013. The workshop was attended by a multi-disciplinary team of experts from 16 countries and three international institutions. The book identifies the state-of-the-art tools and processes being used for cyber defense and highlights gaps in the technology. It presents the best practice of industry and government for incident detection and response and examines indicators and metrics for progress along the security continuum.This book provides those operators and decision makers whose work it is to strengthen the cyber defenses of the global community with genuine tools and expert advice. Keeping pace and deploying advanced process or technology is only possible when you know what is available. This book shows what is possible and available today for computer network defense and for incident detection and response.

Russia has deployed cyber operations to interfere in foreign elections, launch disinformation campaigns, and cripple neighboring states—all while maintaining a thin veneer of deniability and avoiding strikes that cross the line into acts of war. How should a targeted nation respond? In Russian Cyber Operations, Scott Jasper dives into the legal and technical maneuvers of Russian cyber strategies, proposing that nations develop solutions for resilience to withstand future attacks. Jasper examines the place of cyber operations within Russia’s asymmetric arsenal and its use of hybrid and information warfare, considering examples from recent French and US presidential elections and the 2017 NotPetya mock ransomware attack, among others. Jasper shows the international effort to counter these operations through sanctions and

indictments has done little to alter Moscow’s behavior and instead proposes that nations use data correlation technologies in an integrated security platform to establish a more resilient defense. Russian Cyber Operations provides a critical framework for determining whether Russian cyber campaigns and incidents rise to the level of armed conflict or operate at a lower level as a component of competition. Jasper’s work offers the national security community a robust plan of action critical to effectively mounting a durable defense against Russian cyber campaigns.

International cooperation and international relations with regards to cyberspace Technical challenges and requirements Conflict in cyberspace Regulations and standards Virtualisation

Peacetime Regime for State Activities in Cyberspace
Tallinn Manual on the International Law Applicable to Cyber Warfare
Public International Law of Cyberspace
Strengthening Maritime Security Through Cooperation
Best Practices in Computer Network Defense: Incident Detection and Response
Fourth Edition
Cyber Operations and International Law
2015 7th International Conference on Cyber Conflict Architectures in Cyberspace (CyCon)
Report
NATO CCD COE Workshop on 'ethics and Policies for Cyber Warfare' (Magdalen College, Oxford)

In today s increasingly complex cyberspace we see a variety of actors struggling to gain or maintain their position The ubiquitous use of information and communication technologies has had a profound influence on how these actors pursue their goals and interests The 8th International Conference on Cyber Conflict (CyCon 2016) will focus on cyber power as one of the core elements of relations between different stakeholders and will discuss how the traditional concept of power applies to cyberspace Both hard and soft power are being employed to achieve strategic and political goals through technical, legal and economic means But how can we assess such power? How can we ensure that such power remains in the right hands? How can we ensure or enforce cyber power without risking conflict escalation? How can we respond to exercises of this power with the right tools and measures? Is there a way to maintain a balance of power in cyberspace?

"What, exactly, is 'National Cyber Security'? The rise of cyberspace as a field of human endeavour is probably nothing less than one of the most significant developments in world history. Cyberspace already directly impacts every facet of human existence including economic, social, cultural and political developments, and the rate of change is not likely to stop anytime soon. However, the socio-political answers to the questions posed by the rise of cyberspace often significantly lag behind the rate of technological change. One of the fields most challenged by this development is that of 'national security'. The National Cyber Security Framework Manual provides detailed background information and in-depth theoretical frameworks to help the reader understand the various facets of National Cyber Security, according to different levels of public policy formulation. The four levels of government--political, strategic, operational and tactical/technical--each have their own perspectives on National Cyber Security, and each is addressed in individual sections within the Manual. Additionally, the Manual gives examples of relevant institutions in National Cyber Security, from top-level policy coordination bodies down to cyber crisis management structures and similar institutions."--Page 4 of cover.

Recent cyber security related discussions in international forums indicate 'cyber norms' or cyber 'norms of behaviour' as the most suitable vehicles for guiding states' behaviour in cyberspace. The main goals for agreeing on norms are believed to include increased predictability, trust and stability in the use of ICTs, hopefully steering states clear of possible coflict due to misunderstandings. Additionally, norms are seen as guiding principles for shaping domestic and foreign policy as well as a basis for forging international partnerships. of a series of workshops organised by the NATO CCD COE during 2014- 2015.1 The aim of the collection of articles is to shed light on the different approaches to 'cyber norms' in various research domains. The articles outline how different disciplines define, prioritise and promote norms, and suggest approaches for developing cyber norms. We hope that the specific angles from which our distinguished authors tackle cyber norms will benefit the research community as well as explain the difficulties related to agreeing on common cyber norms. As our book focuses mainly on international cyber norms that aim to regulate malicious or potentially harmful cyber activities between states, this introductory article paves the way for the following chapters of the book by giving an overview of the main international platforms where the most advanced cyber powers have addressed the subject.

This book presents 12 essays that focus on the analysis of the problems prompted by cyber operations (COs). It clarifies and discusses the ethical and regulatory problems raised by the deployment of cyber capabilities by a state’s army to inflict disruption or damage to an adversary’s targets in or through cyberspace. Written by world-leading philosophers, ethicists, policy-makers, and law and military experts, the essays cover such topics as the conceptual novelty of COs and the ethical problems that this engenders; the applicability of existing conceptual and regulatory frameworks to COs deployed in case of conflicts; the definition of deterrence strategies involving COs; and the analysis of models to foster cooperation in managing cyber crises. Each essay is an invited contribution or a revised version of a paper originally presented at the workshop on Ethics and Policies for Cyber Warfare, organized by the NATO Cooperative Cyber Defence Centre of Excellence in collaboration with the University of Oxford. The volume endorses a multi-disciplinary approach, as such it offers a comprehensive overview of the ethical, legal, and policy problems posed by COs and of the different approaches and methods that can be used to solve them. It will appeal to a wide readership, including ethicists, philosophers, military experts, strategy planners, and law- and policy-makers.

The result of a three-year project, this manual addresses the entire spectrum of international legal issues raised by cyber warfare.

Attitudes, Strategies, Organisation
Russian Cyber Operations

Ethics and Policies for Cyber Operations
2012 4th International Conference on Cyber Conflict (CYCON 2012)
International Cyber Norms
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence
Tallinn, Estonia, 5 - 8 June 2012
National Cyber Security Organisation, Italy
National Cyber Security Organisation, Czech Republic
NATO Cyberspace Capability

The founding principles of North Atlantic Treaty Organization (NATO) were the collective defense, crisis management, and cooperative security amongst its member countries. Conceived in a Cold War environment, the Alliance has endured strategic changes through major conflicts and global power shifts that eventually led to the fall of the Warsaw Pact. After a brief period where some pundits questioned its relevancy, NATO has experienced a renaissance of its core security functions with the adoption of a new Strategic Concept in 2010. The development of cyberspace defense capabilities for NATO has been making steady progress since its formal introduction at the North Atlantic Council Prague Summit in 2002. Bolstered by numerous cyber attacks such as those in Estonia in 2007, Alliance priorities were formalized in subsequent NATO cyber defense policies that were adopted in 2008, 2011, and 2014. This monograph examines the past and current state of NATO's cyberspace defense efforts by assessing the appropriateness and sufficiency of them to address anticipated threats to member countries, including the United States. This analysis focuses on the recent history of NATO's cyberspace defense efforts and how changes in NATO's strategy and policy writ large embrace the emerging nature of cyberspace for military forces, as well as other elements of power. In general, the topics presented are well documented in many sources. Thus, this monograph serves as a primer for current and future operations and provides senior policymakers, decision-makers, military leaders, and their respective staffs with an overall appreciation of existing capabilities as well as the challenges, opportunities, and risks associated with cyberspace-related operations in the NATO context. The scope of this discussion is limited to unclassified and open source information; any classified discussion must occur within other venues. This monograph has three main sections: NATO Cyberspace Capability: Strategy and Policy. This section examines the evolution of the strategic foundations of NATO cyber activities, policies, and governance as they evolved over the past 13 years. It analyzes the content of the summit meetings of the NATO North Atlantic Council for material related to cyber defense. It also summarizes the evolution of NATO formal cyber defense policy and governance since 2002. NATO Cyberspace Capability: Military Focus. NATO cyber defense mission areas include NATO network protection, shared situational awareness in cyberspace, critical infrastructure protection, counter-terrorism, support to member country cyber capability development, and response to crises related to cyberspace. This section explores these mission areas by examining the operations and planning, doctrine and methods, and training and exercises related to NATO military cyberspace activities. Key Issues for Current Policy. The new Enhanced Cyber Defence Policy affirms the role that NATO cyber defense contributes to the mission of collective defense and embraces the notion that a cyber attack may lead to the invocation of Article 5 actions for the Alliance. Against this backdrop, this section examines the related issues of offensive cyberspace, deterrence in and through cyberspace, legal considerations, and cooperation with the European Union. This monograph concludes with a summary of the main findings from the discussion of NATO cyberspace capabilities and a brief examination of the implications for Department of Defense and Army forces in Europe. Topics include the roles and evolution of doctrine, deterrence, training, and exercise programs, cooperation with industry, and legal standards. NATO cyberspace activities face many challenges that must be assessed and prioritized on a recurring basis by policymakers."

In this volume, contributors from academia, industry, and policy explore the inter-connections among economic development, socio-political democracy and defense and security in the context of a profound transformation, spurred by globalization and supported by the rapid development of information and communication technologies (ICT). This powerful combination of forces is changing the way we live and redefining the way companies conduct business and national governments pursue strategies of innovation, economic growth and diplomacy. Integrating theoretical frameworks, empirical research and case studies, the editors and contributors have organized the chapters into three major sections, focusing on cyber-development, cyber-democracy and cyber-defense. The authors define cyber-development as a set of tools, methodologies and practices that leverage ICT to catalyze and accelerate social, political and economic development, with an emphasis on making the transition to knowledge-based economies. One underlying understanding here is that knowledge, knowledge creation, knowledge production and knowledge application (innovation) behave as crucial drivers for enhancing democracy, society, and the economy. By promoting dissemination and sharing of knowledge, cyber-democracy allows a knowledge conversion of the local into the global (gloCal) and vice versa, resulting in a gloCal platform for communication and knowledge interaction and knowledge enhancement. Meanwhile, technology-enabled interconnectivity increases the need to adopt new methods and actions for protection against existing threats and possible challenges to emerge in the future. The final section contemplates themes of cyber-defense and security, as well as emerging theories and values, legal aspects and trans-continental links (NATO, international organizations and bilateral relations between states). Collectively, the authors present a unique collection of insights and perspectives on the challenges and opportunities inspired by connectivity.

The study outlines the division of cyber security tasks and responsibilities between different agencies, describes their mandate, tasks and competences, and the coordination among them. In particular, it describes the mandates of political and strategic management; operational cyber security capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and crisis management. It also offers a summary of the national information society setting and e-government initiatives as well as the national cyber security strategy objectives in order to clarify the context for the organisational approach in a particular nation.

This compact, highly engaging book examines the international legal regulation of both the conduct of States among themselves and conduct towards individuals, in relation to the use of cyberspace. Chapters introduce the perspectives of various stakeholders and the challenges for international law. The author discusses State responsibility and key cyberspace rights issues, and takes a detailed look at cyber warfare, espionage, crime and terrorism. The work also covers the situation of non-State actors and quasi-State actors (such as IS, or ISIS, or ISIL) and concludes with a consideration of future prospects for the international law of cyberspace. Readers may explore international rules in the areas of jurisdiction of States in cyberspace, responsibility of States for cyber activities, human rights in the cyber world, permissible responses to cyber attacks, and more. Other topics addressed include the rules of engagement in cyber warfare, suppression of cyber crimes, permissible limits of cyber espionage, and suppression of cyber-related terrorism. Chapters feature explanations of case law from various jurisdictions, against the background of real-life cyber-related incidents across the globe. Written by an internationally recognized practitioner in the field, the book objectively guides readers through on-going debates on cyber-related issues against the background of international law. This book is very accessibly written and is an enlightening read. It will appeal to a wide audience, from international lawyers to students of international law, military strategists, law enforcement officers, policy makers and the lay person.

Cyber weapons and the possibility of cyber conflict—including interference in foreign political campaigns, industrial sabotage, attacks on infrastructure, and combined military campaigns—require policymakers, scholars, and citizens to rethink twenty-first-century warfare. Yet because cyber capabilities are so new and continually developing, there is little agreement about how they will be deployed, how effective they can be, and how they can be managed. Written by leading scholars, the fourteen case studies in this volume will help policymakers, scholars, and students make sense of contemporary cyber conflict through historical analogies to past military-technological problems. The chapters are divided into three groups. The first—What Are Cyber Weapons Like?—examines the characteristics of cyber capabilities and how their use for intelligence gathering, signaling, and precision striking compares with earlier technologies for such missions. The second section—What Might Cyber Wars Be Like?—explores how lessons from several wars since the early nineteenth

century, including the World Wars, could apply—or not—to cyber conflict in the twenty-first century. The final section—What Is Preventing and/or Managing Cyber Conflict Like?—offers lessons from past cases of managing threatening actors and technologies.

Strategic Cyber Security
National Cyber Security Framework Manual
Coding the Boundaries of Conflict
Fourteen Analogies
National Cyber Security Organisation, Spain
NATO's New Strategic Concept. A Comprehensive Assessment
Cyber-Development, Cyber-Democracy and Cyber-Defense
International Cyber Incidents
Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
2016 8th International Conference on Cyber Conflict (CyCon)

NATO Cooperative Cyber Defence Centre of Excellence has published the "National Cyber Security Framework Manual" which aims to support NATO Member States and Partner Nations as a guide on how to develop or improve their national policies and laws of national cyber security. The Manual is not attempting to provide a single universally applicable check-list of aspects to consider when drafting a national cyber security strategy. Rather, it provides detailed background information and in-depth theoretical frameworks to help the reader understand the different facets of national cyber security, according to different levels of public policy formulation. The four levels of government - political, strategic, operational and tactical/technical - each have their own perspectives on national cyber security, and each is addressed in individual sections within the Manual. Additionally, the Manual gives examples of relevant institutions in national cyber security, from top-level policy coordination bodies down to cyber crisis management structures and similar institutions. The new edition of the highly influential Tallinn Manual, which outlines public international law as it applies to cyber operations.

National cyber security : framework manual
National Cyber Security Organisation, the Netherlands
A NATO Cooperative Cyber Defence Centre of Excellence Initiative
International Law, International Relations and Diplomacy
National Cyber Security Organisation, Lithuania
National Cyber Security Organisation, Poland
A Strategic and Operational Evolution
Challenges, Opportunities and Implications for Theory, Policy and Practice