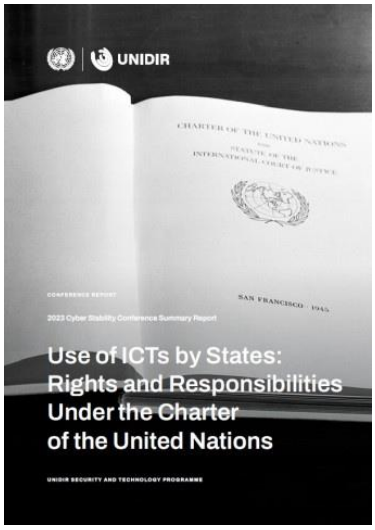
UNIDIR Publications on International Cyber Security

1. **Use of ICTs by States: Rights and Responsibilities Under the UN Charter**

2023
https://unidir.org/publication/use-icts-states-rights-and-responsibilities-under-un-charter

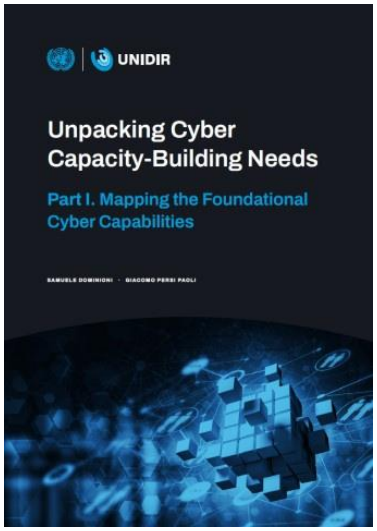


The Cyber Stability Conference 2023 provided a platform for a substantive discussion on the application of the law of the Charter of the United Nations in the context of State conduct using information and communications technologies (ICTs). Specifically, the Conference deliberated on four areas of the law—use of force, armed attack and self-defence, role and powers of the Security Council, and peaceful settlement of disputes—with panellists, State representatives, focusing in their interventions on national interpretations of the law and State practice.

This report provides a summary of the Conference briefings and discussions, an outline of the emerging convergent and divergent positions, as well as several suggestions for how to advance multilateral discussions on the application of international law to State conduct using ICTs and to ensure rule of international law in the twenty-first century. As such, the report charts the potential focus areas for future multilateral deliberations on the Charter and the use of ICTs in the context of international peace and security.

2. **Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities**

2023
https://unidir.org/publication/unpacking-cyber-capacity-building-needs-part-i-mapping-foundational-cyber-capabilities



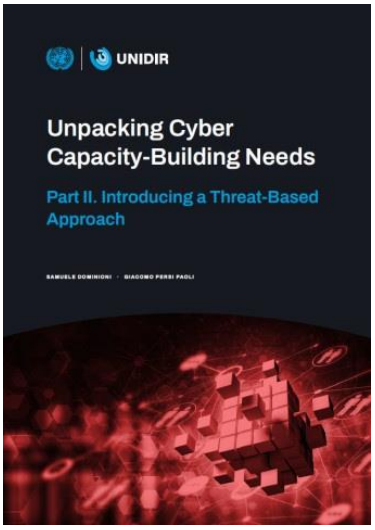
There is a growing emphasis among Member States on the need to support the implementation of the Framework for Responsible State Behaviour in the ICT environment (the Framework), including through dedicated guidance, assistance, and dedicated capacity-building efforts. In response to this demand and to increase the cybersecurity and resilience of Member States, the UNIDIR Security and Technology programme conducted a research study with three main objectives, which are to identify foundational cyber capabilities, strengthen States' ability to effectively prevent or mitigate the impact of selected malicious ICT activities, and design a tool to better identify requirements and prioritize capacity-building interventions.

The outcomes of the research project can be found in these two publications. The first report, Part I. Mapping the Foundational Cyber Capabilities, is centered on

the concept of Foundational Cyber Capabilities (FCCs), which are defined as the combination of policies and regulations, processes and structures, partnerships and networks, people and skills, and technology necessary to implement the Framework.

3. **Unpacking Cyber Capacity-Building Needs: Part II. Introducing a Threat-Based Approach**

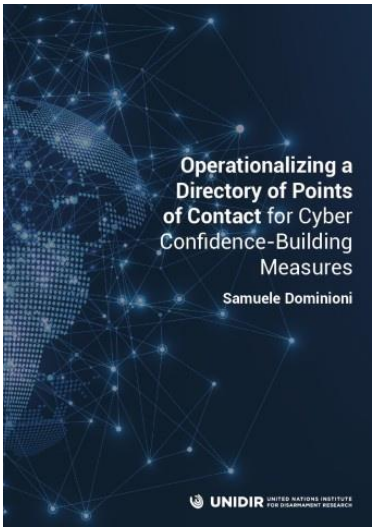
2023
https://unidir.org/publication/unpacking-cyber-capacity-building-needs-part-ii-introducing-threat-based-approach



The second report, Part II. Introducing a Threat-Based Approach, proposes an approach that would allow governments to better assess their readiness to leverage the Framework to prevent or respond to specific malicious ICT activities and threats.

4. **Operationalizing a Directory of Points of Contact for Cyber Confidence-Building Measures**

2023
https://unidir.org/publication/operationalizing-directory-points-contact-cyber-confidence-building-measures



This report supports substantive deliberations, and facilitates the progress of the Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security by elaborating possible options and practical recommendations for establishing an effective global directory of Points of Contact (PoC) on security in the use of ICTs. It also serves as a reference study on procedures, parameters, and practices (including lessons learned) of existing PoC directories and networks in the field of disarmament and cyber.

5. **Towards a More Stable and Secure ICT Environment: Unpacking Inter-State Cooperation (Conference Summary Report)**

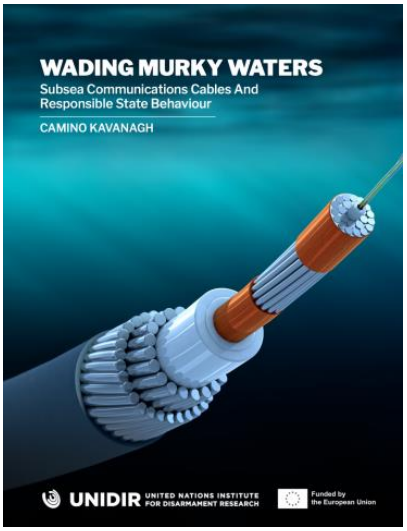
2023
https://unidir.org/publication/towards-more-stable-and-secure-ict-environment-unpacking-inter-state-cooperation

This report provides a brief summary of the substantive discussions during the "Towards a More Stable and Secure ICT Environment: Unpacking Inter-State Cooperation" conference held in Geneva on 2 December 2022.

The conference provided a platform for structured discussion among State representatives on good practices in the field of inter-State cooperation and the relevant confidence- and capacity-building measures for more peaceful and stable international ICT environment.

6. **Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour**

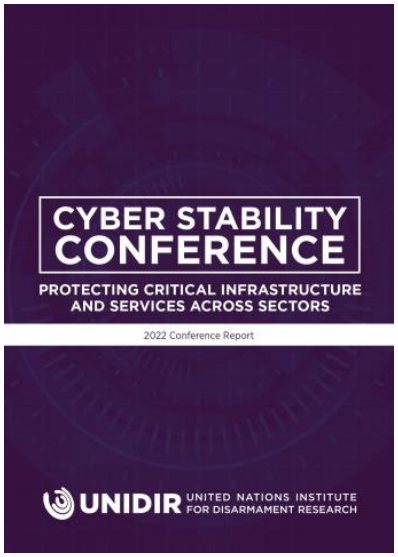
2023
https://unidir.org/publication/wading-murky-waters-subsea-communications-cables-and-responsible-state-behaviour



This report approaches subsea communications cables from a systemic perspective: as core elements of the broader ICT ecosystem. It begins with an overview of developments i subsea cable technology and associated 'wet' (undersea) and 'dry' (land) plant infrastructure and the main actors involved in the subsea cable industry. It then provides an overview of the more commonly cited threats and vulnerabilities relevant to subsea cable systems and related infrastructure, followed by an introduction to the extant subsea cable governance regime. Drawing in part from the Government Best Practices of the International Cable Protection Committee and existing recommendations negotiated under the umbrella of the General Assembly's First Committee on Disarmament and International Security, it concludes with some preliminary recommendations on cooperative steps that governments can take to advance responsible State behaviour and to strengthen the resilience of subsea cable systems and related infrastructure.

7. 2022 Cyber Stability Conference: Protecting Critical Infrastructure and Services Across Sectors

2022
https://unidir.org/publication/cyber-stability-conference-protecting-critical-infrastructure-and-services-across

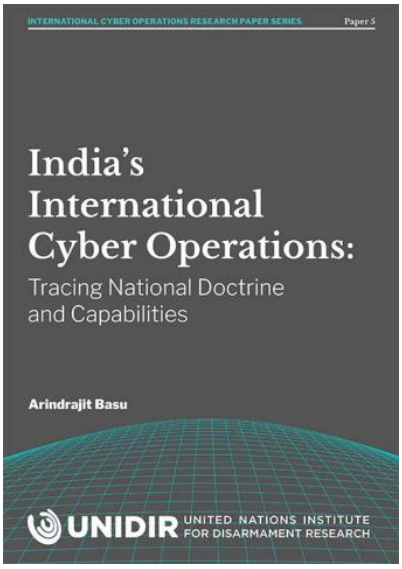


This report provides a short summary of the 2022 edition of UNIDIR's Cyber Stability Conference (CS2022) held in Geneva on 5 July 2022. The event focused on discussing the protection of critical infrastructure and critical information infrastructure supporting essential services to the public.The conference convened representatives from international organizations, industry, governments, and civil society to reflect on how to further progress in multilateral discussions and support more efficient policy interventions by national governments for critical infrastructure protection.

8. India's International Cyber Operations: Tracing National Doctrine and Capabilities

International Cyber Operations: National Doctrines and Capabilities Series

2022
https://unidir.org/cyberdoctrines/India



Cybersecurity has been recognized by Indian decision makers as a key foreign policy and security priority. However, at this stage, there has been no clear public articulation of any intention by India to conduct international cyber operations. There is no publicly known overarching declaratory doctrine, policy or legislative framework that captures India's strategic interests, ambitions and restraints in this arena. However, the cyber institutional machinery and policy landscape are evolving rapidly, with several new institutions set up in the last decade and several policies in the nascent stages of development or due to be released soon, most notably the National Cyber Security Strategy. Further, public statements by public officials on India's cyber doctrine and operations could serve as evidence of intent to conduct international cyber operations.

Therefore, at this stage, India's present capabilities and strategy can be inferred from an informed analysis of existing State practice and institutional architecture and a combined reading of existing laws and policies. However, India's approach to cybersecurity is rooted in its appraisal of strategic interests. As these interests and threats evolve, India may more proactively disclose capabilities and frame a governing doctrine in order to robustly project power in cyberspace.

9. A Taxonomy of Malicious ICT Incidents

2022
https://unidir.org/publication/taxonomy-malicious-ict-incidents

The international community has acknowledged that information communication technology (ICT) developments are providing both States and non-State actors with malicious new methods and uses of ICT.

The UNIDIR Taxonomy of Malicious ICT Incidents is a tool that provides the multistakeholder community with an easy-to-read infographic that can help in analysing malicious ICT incidents. It is designed to work towards a baseline of knowledge and common understanding, which could help the international community to build confidence through increased information-sharing about malicious ICT incidents.

Also available is an Annex to the Taxonomy of Malicious ICT Incidents, which explores other existing taxonomies and classifications upon which the UNIDIR Taxonomy builds and relies.

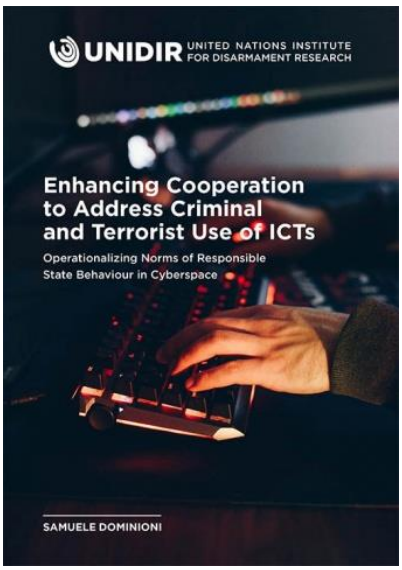
10. 2021 Cyber Stability Conference: Towards a More Secure Cyberspace

2022
https://unidir.org/publication/2021-cyber-stability-conference-towards-more-secure-cyberspace

This report provides a short summary of the 2021 edition of UNIDIR's Cyber Stability Conference (CS2021) held in Geneva on 3 December 2021 The event focused on discussing the progress of the two multilateral United Nations (UN) processes on cyberspace, namely the Group of Governmental Experts on Advancing responsible State behaviors in cyberspace in the context of international security (GGE) and the Open-Ended Working Group in the Field of Information and Telecommunications in the Context of International Security (OEWG). The conference convened representatives from government, industry, and civil society to reflect on how we could build on past successes to advance the agenda for an open, secure, stable, accessible, and peaceful ICT environment.

11. Enhancing Cooperation to Address Criminal and Terrorist Use of ICTs

2022
https://unidir.org/publication/enhancing-cooperation-address-criminal-and-terrorist-use-icts



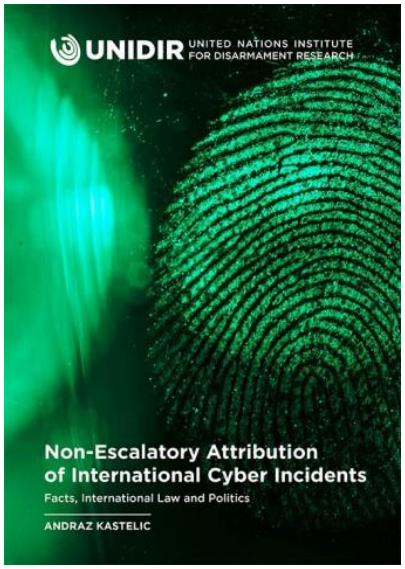
The increasing magnitude and sophistication of criminal and terrorist use of ICTs could be seen as a threat to international security. Because of the transnational dimension of these threats, effective cooperation among States is vital.

In 2015 the United Nations General Assembly approved Resolution 70/237 to welcome the 2015 report of the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, which proposed a set of 11 voluntarily non-binding norms.

Among these was Norm 13 D, which invited States to cooperate to address criminal and terrorist use of ICTs. This report identifies challenges and possible solutions by proposing actionable options for States, particularly in the area of information exchange and handling of electronic evidence for international investigations and prosecutions.

12. Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics

2022
https://www.unidir.org/attribution



Attribution – the process of allocating responsibility for a malicious cyber operation – is comprised of three distinct and intertwined aspects: factual or technical, legal, and political. This paper analyses these three aspects through the prism of the normative expectations of responsible State behaviour in cyberspace. The paper goes on to make a number of suggestions of how to consider the challenges of attribution and how to operationalize norm B of the 2015 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

13. **Due Diligence in Cyberspace: Normative Expectations of Reciprocal Protection of International Legal Rights**

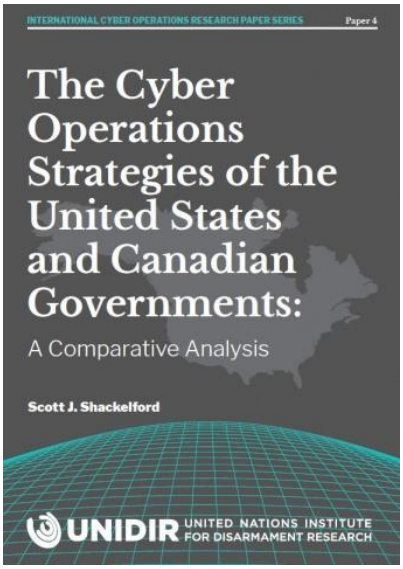
2021
https://www.unidir.org/duediligence

Noting the ability of voluntary norms to strengthen peace, security, and stability in international relations, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) proposed a normative framework of mutual international assurance, based on the due diligence principle of international law. This paper provides an exposition of the divergences and convergences in national interpretations of the norm C, as formulated in the 2015 GGE report and later elaborated in the 2021 report, which suggests that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs". As elaborated by this paper, States are yet to reach an agreement on the scope of the norm, knowledge conditions, standards, and thresholds of the norm. What is more, States have divergent positions on whether it is a voluntary norm, a rule or a principle of international law imposing certain obligations.

14. **The Cyber Operations Strategies of the United States and Canadian Governments: A Comparative Analysis**

International Cyber Operations: National Doctrines and Capabilities Series

2021
https://www.unidir.org/cyberdoctrines/US-Canada



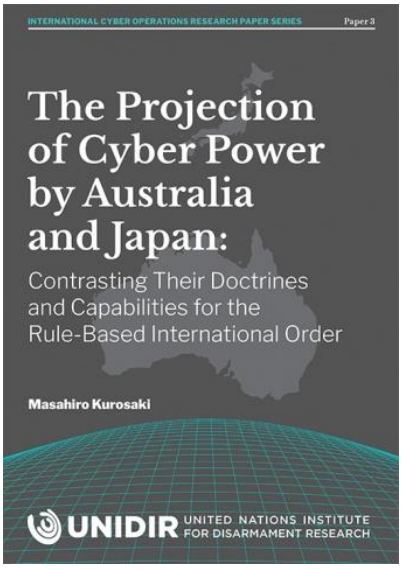
This fourth paper in the International Cyber Operations Research Paper Series analyses the cybersecurity strategies of the United States and Canada, including their treatment of so-called offensive cyber operations and relevant national doctrines pertaining to active defence and self-defence.

To better inform conclusions, the concept of offensive cyber operation is interpreted broadly, incorporating relevant strategies and – where necessary – the policy statements, manuals and legislation of each State. Particular attention is also paid to the role of international law and emerging cyber norms in guiding State practice relating to cyber operations in both countries.

15. The Projection of Cyber Power by Australia and Japan: Contrasting Their Doctrines and Capabilities for the Rule-Based International Order

International Cyber Operations: National Doctrines and Capabilities Series

2021
https://www.unidir.org/cyberdoctrines/Australia-Japan



This third paper in the International Cyber Operations Research Paper Series offers an analysis of how and under what guidance Australia and Japan now seek to build and employ their offensive cyber capabilities – the capabilities to disrupt, degrade, or deny a targeted computer system or network – to project their power outward across the region. In doing so, it offers the following observations:

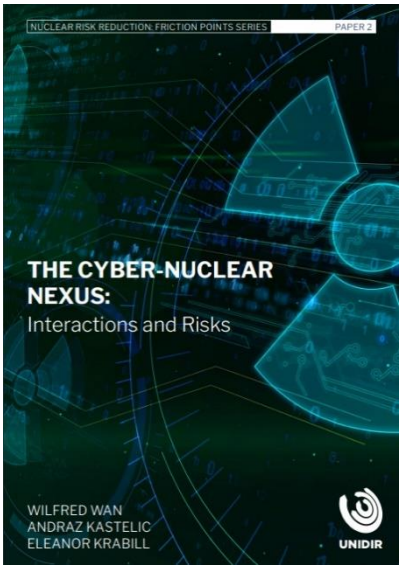
First, Australia has been advancing its offensive cyber capabilities with an eye on a full spectrum of situations covering "grey-zone" activities prevalent in the Indo-Pacific. These capabilities are housed in its major intelligence agency and are intended to discourage offshore malicious actors from targeting its networks in violation of cyber norms.

Second, Japan has limited its external cyber capabilities to responses by its armed forces and to situations of an armed attack.

Third, notwithstanding the importance of a collective approach to filling gaps in cyber capabilities between Australia and Japan, there is growing divergence between like-minded States over the applicability of some rules of international law to cyberspace – notably the principles of sovereignty and due diligence. This could have an adverse effect on their willingness to take concerted and effective cyber measures against the growing "grey-zone" cyber activities in the region.

16. The Cyber-Nuclear Nexus: Interactions and Risks

2021
https://www.unidir.org/publication/cyber-nuclear-nexus-interactions-and-risks



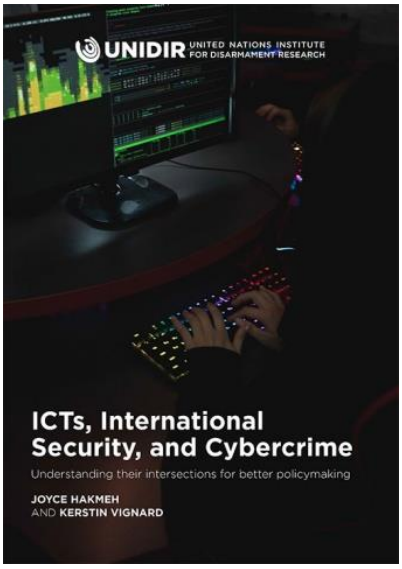
This publication is the second in a series that profiles different "friction points" among nuclear armed and nuclear-allied States, examining issues of contention in their relations that can spark potential conflict and nuclear escalation.

It traces trends both in the development of cyber capabilities and the digitalization of nuclear weapons systems that could drive more frequent interactions at the cyber–nuclear nexus. It considers how these interactions, direct and indirect, might impact on escalatory risk scenarios—drawing upon State doctrines, postures, and capabilities in the nuclear and cyber spheres. It then outlines a series of recommendations for States both to minimize cyber–nuclear interactions and to mitigate their effects when they do occur.

As part of UNIDIR's ongoing research on nuclear risk reduction, this paper is intended to feed into the dialogue on taking forward risk reduction—and on the development of practical and feasible measures that can help to close pathways to use.

17. ICTs, International Security, and Cybercrime

2021
www.unidir.org/publication/icts-international-security-and-cybercrime

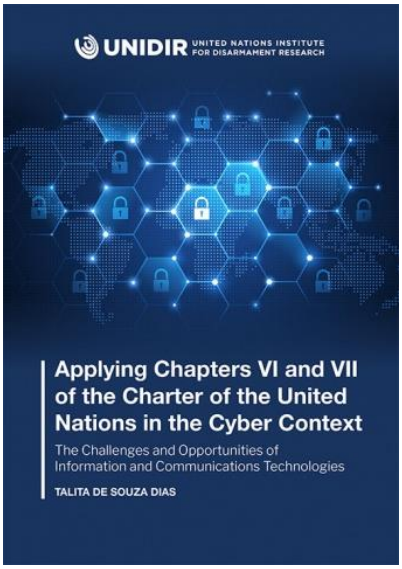


Information and Communication Technologies (ICTs) can be exploited for criminal purposes (through cybercrime) or used to undermine international security (through so-called cyberattacks or cyber operations). However, the international security and crime dimensions of ICTs are distinct issues, with different processes, tools and frameworks designed to address them, even if they do increasingly overlap in some ways.

In this context, there is a need for greater understanding of how international frameworks and policy discussions on combatting cybercrime and promoting responsible State behaviour in the use of ICTs may be better leveraged in formulating coherent responses.

18. Applying Chapters VI and VII of the Charter of the United Nations in the Cyber Context

2021
www.unidir.org/publication/applying-chapters-vi-and-vii-charter-united-nations-cyber-context



How can Chapters VI and VII of the UN Charter be used to restore peace and security following an international cyber incident?

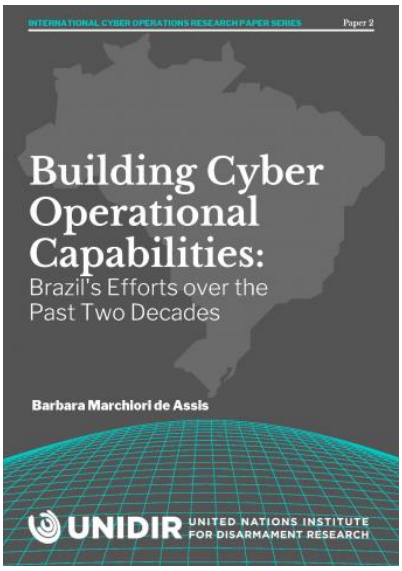
International law as a whole, and the Charter of the United Nations in particular, applies to information and communications technologies (ICTs) and the digital environments that they enable. To address cyber events constituting disputes likely to endanger the maintenance of international peace and security; situations which might lead to international friction or give rise to a dispute under Chapter VI; and threats to the peace, breaches of the peace, or acts of aggression under Chapter VII, traditional dispute settlement and enforcement measures could be complemented or replaced with new, ICT-specific measures.

19. Building Cyber Operational Capabilities: Brazil´s Efforts over the Past Two Decades

International Cyber Operations: National Doctrines and Capabilities Series

2021

www.unidir.org/cyberdoctrines/Brazil

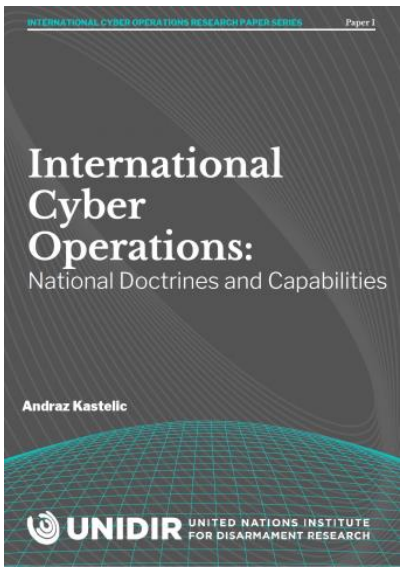


This paper describes the evolution of cyber defence in Brazil, from early discussions in the 2000s to specific policies and measures implemented to develop the national capability to conduct international cyber operations if necessary. Although Brazil has been strengthening its cyber defence capacity for the past two decades, the major international events hosted by the country from 2012 to 2016, such as the World Cup and the Olympic Games, marked a watershed in Brazil's cyber defence capacity development. During this period, not only did Brazil solidify its cyber defence military structure, it also developed a cyber defence doctrine aimed at unifying concepts and guiding operations in cyberspace.

20. International Cyber Operations: National Doctrines and Capabilities Research Papers Series

2021

www.unidir.org/cyberdoctrines



The number of States possessing the capability to conduct international cyber operations against or through foreign information and communications technology (ICT) infrastructure is on the rise. These cyber operations can signal a mounting large-scale threat to the security of a State, could be understood as a violation of sovereignty and may lead to an escalation.

To facilitate transparency, advance trust among States and thus promote stability in international cyberspace, the UNIDIR Security and Technology Programme commissioned a series of research papers outlining national capabilities to conduct international cyber operations and relevant national doctrines regulating the conduct of such operations. In the resulting papers, nine scholars and practitioners provide an overview of capabilities and doctrines pertaining to 15 countries across different regions: Australia, Brazil, Canada, China, France, Germany, India, the Islamic Republic of Iran, Israel, Japan, the Republic of Korea, the Russian Federation, Saudi Arabia, the United *Kingdom of Great Britain and Northern Ireland, and the United States of America. This paper serves as an introduction to the series. It offers contextual background, defines some of the key concepts and sets the methodological boundaries of the series.*

21. International Cooperation to Mitigate Cyber Operations against Critical Infrastructure: Normative Expectations and Emerging Good Practices

2021
www.unidir.org/criticalinfrastructure

Malicious cyber operations pose a threat to critical infrastructure and thus to the well-being of our societies. Major incidents have the potential to both destabilize States and endanger international peace and security. To address the risk of increasingly complex and effective cyber threats aimed at critical infrastructure, the international community uses norms of expected behaviour of States in cyberspace to promote cooperation. This report investigates the norm – as proposed in 2015 by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – that urges States to respond to other States' requests for assistance or mitigation in the event of malicious cyber operations against critical infrastructure.

This publication is also available in Arabic, Chinese and Spanish:

Arabic: https://unidir.org/sites/default/files/2022-02/UNIDIR_International_Cooperation_Mitigate_Cyber_Operations_Critical_Infrastructure_AR.pdf

Chinese: https://unidir.org/sites/default/files/2022-02/UNIDIR_International_Cooperation_Mitigate_Cyber_Operations_Critical_Infrastructure_ZH.pdf

Spanish: https://unidir.org/sites/default/files/2022-03/UNIDIR_Cooperacion_internacional_mitigar_operaciones_ciberneticas_infraestructura_critica.pdf

22. System Update: Towards a Women, Peace and Cybersecurity Agenda

2021
https://www.unidir.org/publication/system-update-towards-women-peace-and-cybersecurity-agenda

System Update explores the relationship between the Women, Peace and Security (WPS) agenda on the one hand and cyber-enabled threats and cybersecurity on the other.

The paper analyses the linkages between WPS priority themes—gender equality, women's participation in international security, prevention and protection of violence against women, gender-differentiated needs—and international cybersecurity. It identifies priority areas that should be addressed to ensure a gender-inclusive cyberspace that protects the rights of women and girls.

23. Gender approaches to cybersecurity: design, defence and response

2021
https://unidir.org/publication/gender-approaches-cybersecurity

Gender approaches to cybersecurity explores how gender norms shape specific activities pertaining to cybersecurity design, defence and response. In each of these three pillars, the research identifies distinct dimensions of cyber-related activities that have gendered implications and, thus, need to be considered from a gender perspective.

The report proposes recommendations for the incorporation of gender considerations throughout international cybersecurity policy and practice, so as to ensure that cybersecurity improves the security of people of all gender identities and expressions, as well as international peace and security. The ultimate conclusion is that these two levels of security cannot be separated.

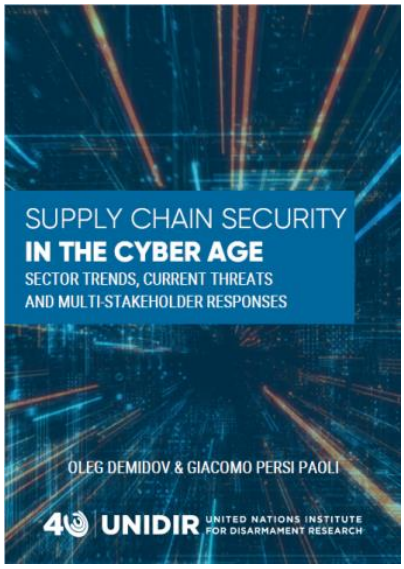
24. 2020 Cyber Stability Conference Report: Exploring the Future of Institutional Dialogue

2020
www.unidir.org/publication/2020-cyber-stability-conference-future-dialogue

This report provides a short summary of the 2020 edition of UNIDIR's Cyber Stability Conference (CS2020) held in Geneva on 28 September 2020 with a focus on the future of institutional dialogue relevant to ICT and international security and stability. CS2020 sought to identify lessons from dialogues that have emerged on other issues of global concern. With an eye to the future of dialogue, speakers discussed issues such as the urgency, purposes and goals of dialogue relevant to ICT and international security. They also addressed more practical questions relating to process design and assessment of outcomes and to ensuring inclusivity in dialogue.

25. Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses

2019
www.unidir.org/publication/supply-chain-security-cyber-age-sector-trends-current-threats-and-multi-stakeholder



A supply chain is traditionally understood as a system of organizations, people, technology, activities, information and resources involved in moving a product or service from supplier (producer) to customer. Today, with the advent of global digital transformation, supply chains and the ways they are managed are transforming, with increasing risks and threats to their security and integrity. These trends highlight the increasing need for internationally shared, adoptable and scalable solutions that could reverse or tamp down cyber threats to supply chains through cooperative efforts of governments, industry, the technology community and other stakeholders. Supply chain security is one of the key issues in multilateral norm development processes related to information and communications technology (ICT), and it continues to be a main point of discussion under two new multilateral cyber processes launched in 2018 under the auspices of the United Nations General Assembly: a new United Nations Group of Governmental Experts (GGE) and an Open-ended Working Group (OEWG) focused on developments in the field of ICT in the context of international security. This report aims to assess how normative responses to ICT-related challenges to supply chain security could be further advanced and operationalized. As norms reflect shared expectations, or standards, of appropriate behaviour, identifying opportunities for improving their operationalization requires looking beyond norms themselves and

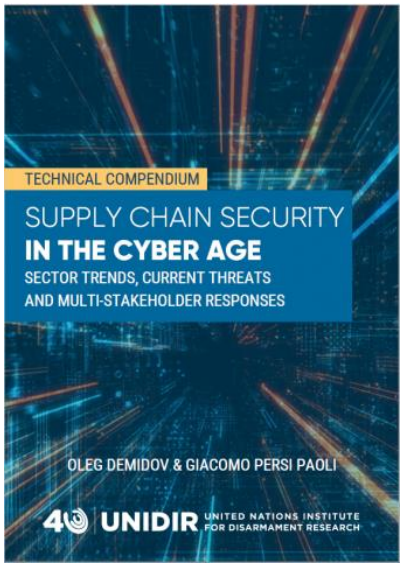
contextualizing them in the wider ecosystem of responses to supply chain security challenges to identify gaps and areas for improvement.

This publication is also available in Arabic:

https://unidir.org/sites/default/files/2022-03/UNIDIR_Supply_Chain_Security_Cyber_Age_AR.pdf

26. Supply Chain Security in the Cyber Age: Technical Compendium

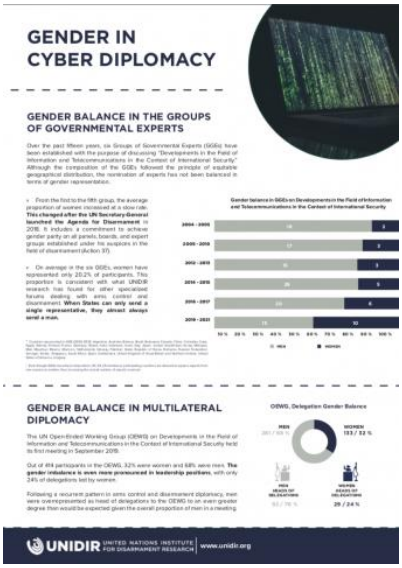
2019
www.unidir.org/publication/supply-chain-security-cyber-age-sector-trends-current-threats-and-multi-stakeholder



This publication is a technical compendium to UNIDIR's report Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses. The compendium is supplementary to the report and provides more detailed information and case-based analysis related to the report's major sections in a number of annexes.

27. Fact Sheet: Gender in Cyber Diplomacy

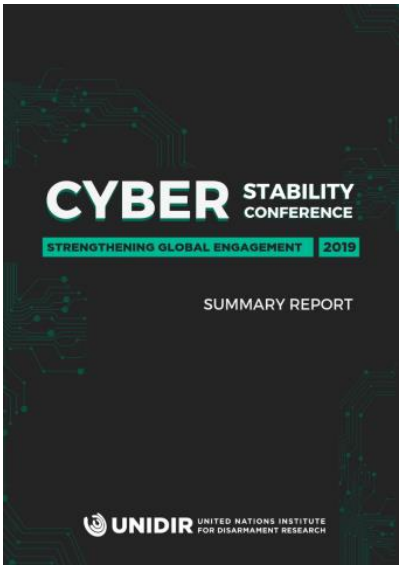
2019
www.unidir.org/publication/fact-sheet-gender-cyber-diplomacy



The factsheet presents numbers on gender balance in cyber diplomacy field and offers ideas to promote gender mainstreaming in cybersecurity discussions.

28. 2019 Cyber Stability Conference Summary Report: Strengthening Global Engagement

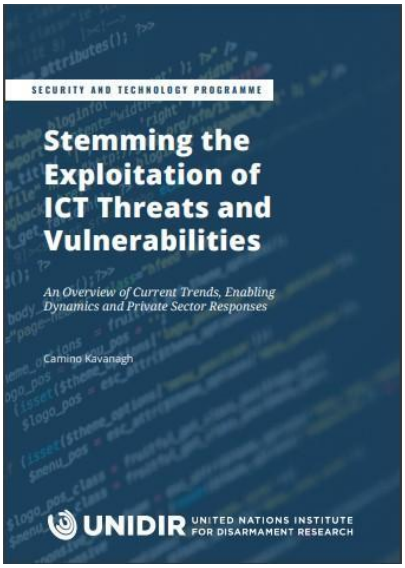
2019
www.unidir.org/publication/cyber-stability-conference-2019-strengthening-global-engagement



The UNIDIR Cyber Stability Conference was held in New York on 6 June 2019. The conference brought together representatives from government, private sector, technical community, academia, and civil society to explore how the GGE and OEWG can advance efforts to promote a secure and stable cyberspace, how multi-stakeholder engagement can contribute to these efforts, and how private sector actors and technical communities can operationalize existing norms; and to map the way forward for ensuring and strengthening cyber stability within the United Nations framework. Participants discussed how both processes can produce complementary outcomes, and how capacity-building can contribute to strengthening global cybersecurity.

29. Stemming the Exploitation of ICT Threats and Vulnerabilities: An Overview of Current Trends, Enabling Dynamics and Private Sector Responses

2019
www.unidir.org/publication/stemming-exploitation-ict-threats-and-vulnerabilities



As societies become increasingly dependent on digital technologies, private technology companies have new roles and responsibilities in regard to shaping and implementing international security policy—particularly in respect to stemming the spread of ICT-related threats and vulnerabilities. This policy brief explores recent trends in threats and vulnerabilities, outlines the dynamics that enable their diffusion, and considers the steps the private sector are taking to address them.

This publication is also available in French:

https://www.unidir.org/publication/limiter-lutilisation-des-fins-malveillantes-des-menaces-et-vulnerabilites-dans-les-tic

30. Electronic and Cyber Warfare in Outer Space

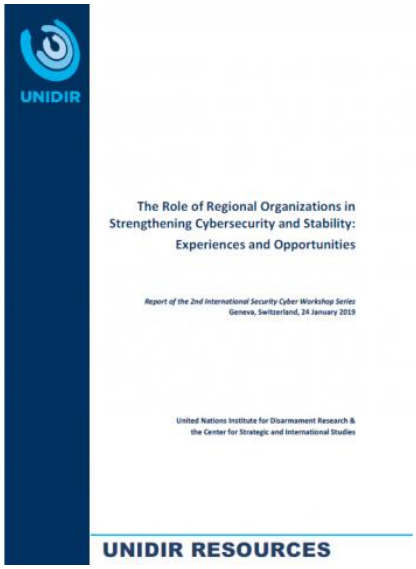
2019
www.unidir.org/publication/electronic-and-cyber-warfare-outer-space

The publication Electronic and Cyber Warfare in Outer Space highlights emerging technologies and capabilities in the electronic and cyber warfare domain as these pertain to outer space and how the international community can address this problem through global governance. Outlining existing counter-space capabilities could establish a sound basis for developing effective measures to address this challenge and prevent dangerous escalation.

31. The Role of Regional Organizations in Strengthening Cybersecurity and Stability: Experiences and Opportunities

Report *of the 2nd International Security Cyber Workshop Series*

Geneva, Switzerland, 24 January 2019
http://www.unidir.org/publication/role-regional-organizations-strengthening-cybersecurity-and-stability

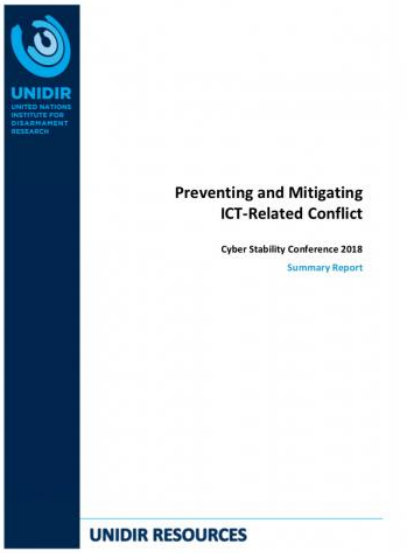


Through a series of regionally focused workshops, the United Nations Institute for Disarmament Research and the Center for Strategic and International Studies are considering regional approaches and perspectives to building cybersecurity.

This workshop, the third in the series, brought together representatives from regional organizations, the private sector, technical organizations, NGOs and academia to consider regional concerns, opportunities and approaches in the context of international peace and security efforts in cyberspace.

32. 2018 Cyber Stability Conference Summary Report: Preventing and Mitigating ICT-Related Conflict

2018
www.unidir.org/publication/preventing-and-mitigating-ict-related-conflict-cyber-stability-conference-2018-summary

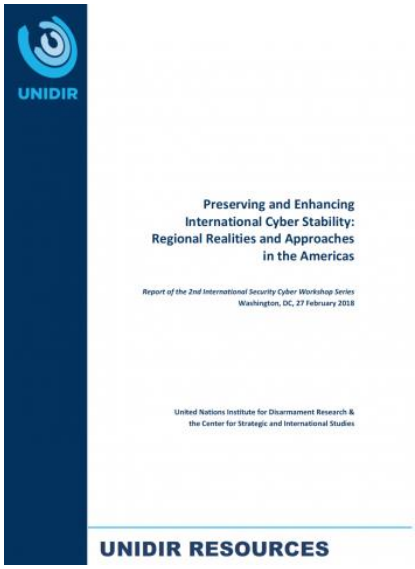


UNIDIR's 2018 Cyber Stability Conference, held in Geneva on 26 September 2018, focused on identifying options and pathways to prevent and mitigate ICT-related conflict. The conference brought together representatives from government, the private sector, academia and civil society to explore current State strategy and practice; developments at regional level; private sector engagement; and prospects for reinvigorating multilateral engagement to address the growing threat of ICT-related conflict. Through the lens of these different topics, the conference looked at the widening gap between our collective aspirations and State practice, identifying different approaches involving different actors to narrowing it.

33. Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches in the Americas

Report of the 2nd International Security Cyber Workshop Series

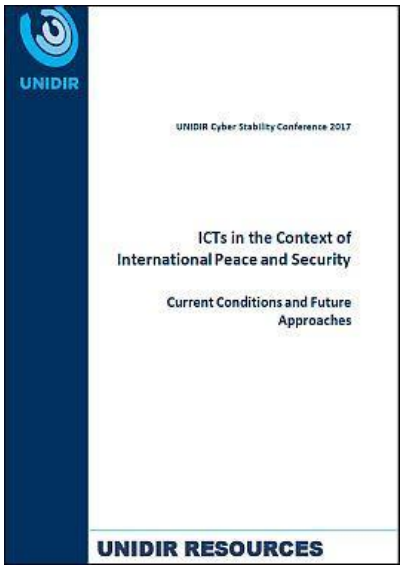
Washington, DC, 27 February 2018
www.unidir.org/publication/preserving-and-enhancing-international-cyber-stability-regional-realities-and



Through a series of regionally focused workshops, the United Nations Institute for Disarmament Research and the Center for Strategic and International Studies are considering regional approaches and perspectives to building cybersecurity. This workshop, the second in the series, brought together members of the Organization of American States with representatives from the private sector, technical organizations, NGOs and academia to consider regional concerns, opportunities and approaches in the context of international peace and security efforts in cyberspace.

34. ICTs in the Context of International Peace and Security: Current Conditions and Future Approaches

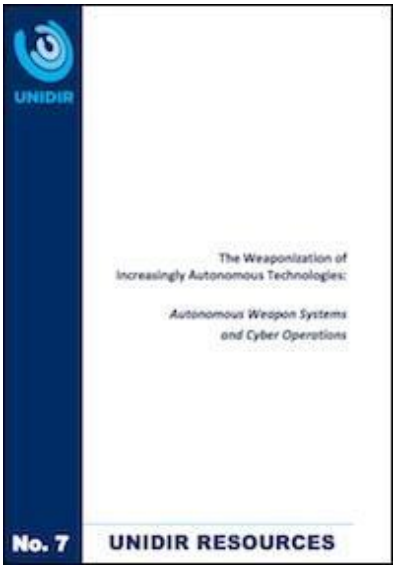
2017
www.unidir.org/publication/icts-context-international-peace-and-security-current-conditions-and-future-approaches



Reports issued in recent years by the United Nations Groups of Governmental Experts (GGEs) on Developments in the Field of Information and Telecommunications in the Context of International Security have been a significant achievement on international security issues in cyberspace. However, the most recent GGE concluded its work in June 2017 without reaching consensus. As Member States will need to consider how best to build upon the last consensus GGE report (2015) in order to promote a peaceful, stable and secure cyber environment for all nations, this year's conference provided an opportunity to take stock and consider next steps for enhancing cyber stability at the international level.

35. The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations

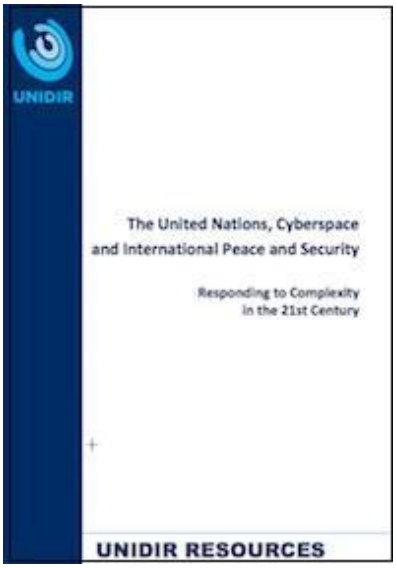
2017
https://unidir.org/publication/weaponization-increasingly-autonomous-technologies-autonomous-weapon-systems-and-cyber



International discussions about autonomous weapons have thus far focused predominantly on conventional weapon systems. These systems are not, however, the only domain in which technological developments in autonomy can have an impact on international security. Rapid advances in machine learning and artificial intelligence also have a significant impact in the field of cyber security, and in particular for offensive operations carried out in cyberspace, so-called "cyber operations". As this paper explains, the interaction of cyber operations and increasingly autonomous physical weapon systems may give rise to new security challenges, as these interactions can multiply complexity and introduce new vulnerabilities.

36. The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century

2017
www.unidir.org/publication/united-nations-cyberspace-and-international-peace-and-security-responding-complexity



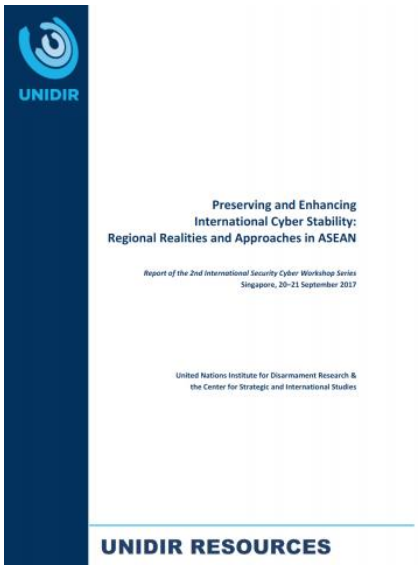
ICT-related issues have been on the agenda of the United Nations for almost two decades, driven by both the positive benefits and the malicious purposes they can be leveraged for. This report is concerned with the UN's response to the latter in the context of international peace and security. It focuses principally on the norm-setting work currently underway within the General Assembly. It outlines where progress has been made in developing a normative framework to shape behaviour in the use of ICTs and ensure stability of the ICT environment, highlighting where challenges and on-going sources of disagreement lie.

The report also discusses linkages and complementarities with other non-UN processes, as well as linkages and complementarities with other items on the UN agenda, directly or indirectly linked to international peace and security. Finally, it identifies how the UN, particularly the UN Secretary-General, might play a role in raising awareness of, supporting and strengthening this on-going work.

37. Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches in ASEAN

Report of the 2nd International Security Cyber Workshop Series

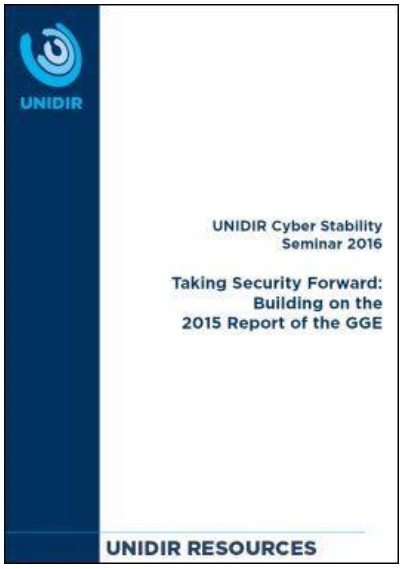
Singapore, 20-21 September 2017
www.unidir.org/publication/preserving-and-enhancing-international-cyber-stability-regional-realities-and-0



Through a series of regionally focused workshops, the United Nations Institute for Disarmament Research and the Center for Strategic and International Studies are considering regional approaches and perspectives to building cybersecurity. This workshop, the first in the series, brought together members of ASEAN and the ASEAN Regional Forum with representatives from the private sector, technical organizations, NGOs and academia to consider regional concerns, opportunities and approaches in the context of international peace and security efforts in cyberspace.

38. UNIDIR Cyber Stability Seminar 2016 - Taking Security Forward: Building on the 2015 Report of the GGE

2016
www.unidir.org/publication/unidir-cyber-stability-seminar-2016-taking-security-forward-building-2015-report-gge

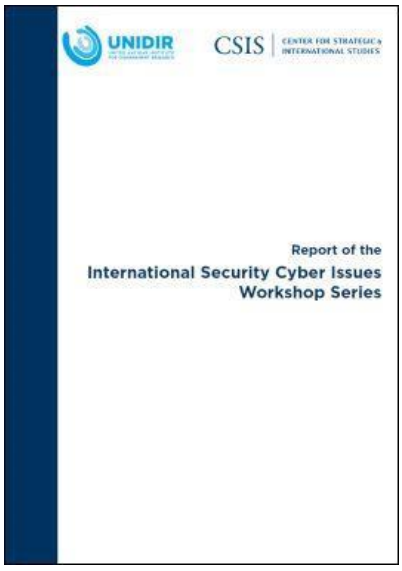


Reports issued in recent years by the United Nations Groups of Governmental Experts (GGEs) on Developments in the Field of Information and Telecommunications in the Context of International Security have significantly altered the political landscape for international cooperation on security issues in cyberspace. The GGE's 2013 Report, which included an agreement among participating states that international law applies in cyberspace, set important precedents for norms and other cooperative measures that will shape future discussion of cybersecurity. More recently, the 2015 Report included a reaffirmation of the applicability of international law, and for the first time, a list of voluntary norms for state in cyberspace during peace time. It also included a norm that "States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions." A new GGE is slated to begin work in August 2016.

This seminar considered how the international community can operationalize and build upon these consensus reports—and generate momentum for a successful 2016-2017 GGE. The seminar brought together stakeholders from the Geneva diplomatic community, industry, and capital-based policymakers to discuss and explore how to leverage the GGE process to promote a peaceful, stable and secure cyber environment.

39. Report of the International Security Cyber Issues Workshop Series

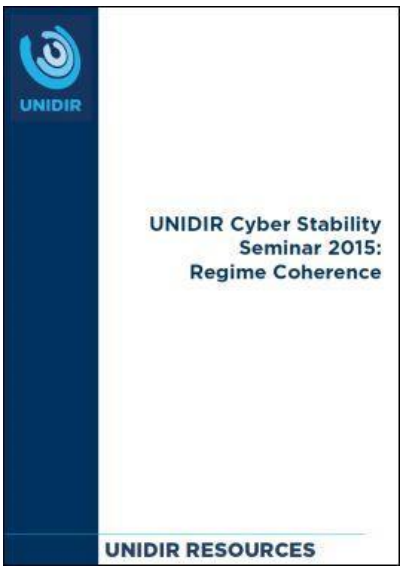
2016
www.unidir.org/publication/report-international-security-cyber-issues-workshop-series



The UN Institute for Disarmament Research and the Center for Strategic and International Studies organized three expert workshops to open and broaden the discussion of international norms for responsible State behaviour in cyberspace and to identify new ideas to support further progress by the international community. The first focused on identification of new norms, the second on the application of international law, and the third on ways to manage the spread of malicious cyber tools. The intent was to build on past progress and to expand the space for international agreement on measures to increase stability and security in cyberspace.

40. UNIDIR Cyber Stability Seminar 2015: Regime Coherence

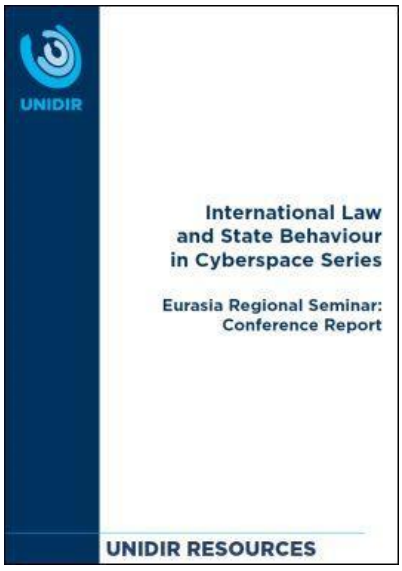
2015
www.unidir.org/publication/unidir-cyber-stability-seminar-2015-regime-coherence



This report reflects the 2015 Cyber Stability conference's aims to support discussions on how current and future norm-setting cyber initiatives can be coordinated to further the development of a pragmatic global approach to cyber stability and avoid being in unintentional conflict with one another. The conference brought together stakeholders from the Geneva diplomatic community, cyber industry, and capital-based policymakers to discuss and explore ways in which the cyber community can better align strategic goals, and promote a stable and secure cyber environment.

41. International Law and State Behaviour in Cyberspace Series. Eurasia Regional Seminar: Conference Report

2015
www.unidir.org/publication/eurasia-regional-seminar-conference-report

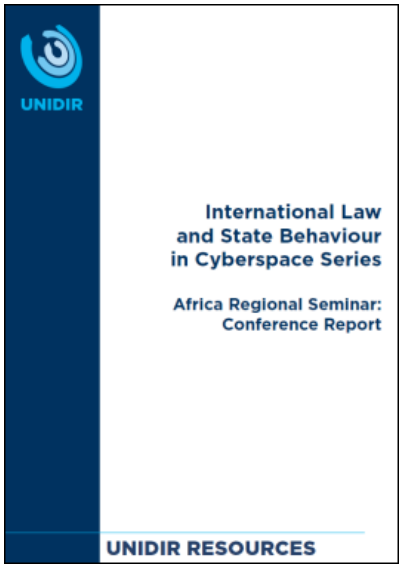


The Eurasia Regional seminar brought together both legal and policy voices to explore the cyber domain's legal context as it relates to the Eurasia region. This meeting provided an opportunity for regional stakeholders to exchange views and opinions, and to engage in a dialogue on the complexities and various interpretations of the applicability of international law in cyberspace within national frameworks. The seminar aimed to promote greater regional understanding, as well as to provide participants with a network of contacts throughout the region that, in the long term, might allow for better communication and cooperation on cyber issues.

42. Africa Regional Seminar: Conference Report

International Law and State Behaviour in Cyberspace Series

2015
www.unidir.org/publication/africa-regional-seminar-conference-report

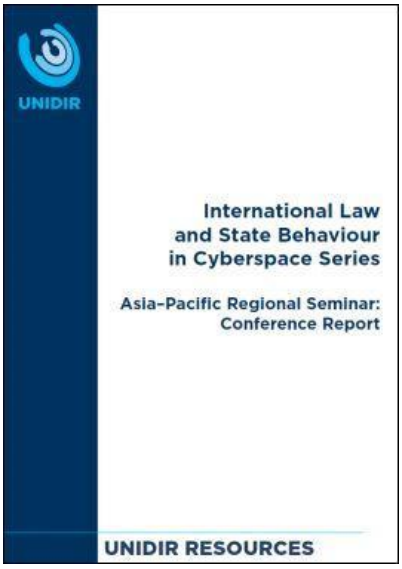


On 3–4 March 2015, the United Nations Institute for Disarmament Research (UNIDIR) carried out the Africa Regional Seminar as part of its International Law and State Behaviour in Cyberspace Series. Held in Nairobi, Republic of Kenya, the Seminar brought together a wide range of government and academic representatives from across the region to discuss some of the key components of international law and its application in the cyber domain.

43. Asia-Pacific Regional Seminar: Conference Report

International Law and State Behaviour in Cyberspace Series

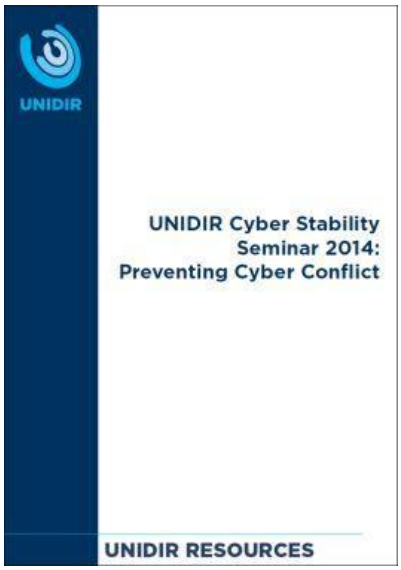
2015
www.unidir.org/publication/asia-pacific-regional-seminar-international-law-and-state-behaviour-cyberspace-series



On 9-10 December 2014, the United Nations Institute for Disarmament Research (UNIDIR) carried out the Asia-Pacific Regional Seminar as part of their International Law and State Behaviour in Cyberspace Series. Held in Seoul, Republic of Korea, the Seminar brought together a wide range of government and academic representatives from across the region to discuss some of the key components of international law and its application in the cyber domain.

44. UNIDIR Cyber Stability Seminar 2014: Preventing Cyber Conflict

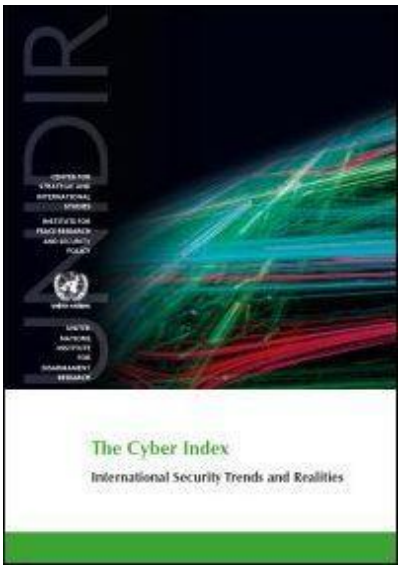
2014
www.unidir.org/publication/unidir-cyber-stability-seminar-2014-preventing-cyber-conflict



The seminar presented an opportunity for states and relevant stakeholders to discuss how to take pragmatic steps towards a more stable and predictable cyber environment. With particular attention paid to the risks of escalation in cyber conflicts, the seminar addressed the growing need to develop mechanisms for discussion, education, and constructive engagement on how to improve cyber stability in the multilateral context.

45. The Cyber Index: International Security Trends and Realities

2013
www.unidir.org/publication/cyber-index-international-security-trends-and-realities



The Cyber Index is intended to serve as a "snapshot" of current cybersecurity activities at the national, regional, and international levels, to help policymakers and diplomats understand the complexity of the arena. In addition, the Index seeks to elucidate some approaches towards mitigating the risks of misperceptions in the cyber domain that threaten to elevate international tensions or perhaps even lead to conflict. The subject matter is multifaceted, highly complicated, and controversial—thus no one study could adequately cover all aspects in depth. Nonetheless, the Cyber Index will help to underpin ongoing discussions and debates by providing facts and fact-based analysis of today's challenges and opportunities regarding international stability and security in the cyber domain.