INTERNATIONAL CYBER OPERATIONS RESEARCH PAPER SERIES Paper 1

International Cyber Operations:

National Doctrines and Capabilities

Andraz Kastelic

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This paper is a product of the Security and Technology Programme's Cyber Stability workstream, which is funded by the Governments of France, Germany, the Netherlands, Norway and Switzerland, and by Microsoft. The author wishes to thank Giacomo Biggio, Renata Hessmann Dalaqua, Masahiro Kurosaki, Giacomo Persi Paoli and Kerstin Vignard for their invaluable advice.

The individual contributions to this series of papers were produced by external consultants, contracted to undertake studies for the Security and Technology Programme. Special gratitude is extended to all the external reviewers who provided their feedback on the individual papers; each of the reviewers is listed with the respective research paper. Design and layout of the publication: Eric M. Schulz.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

About the Author

ANDRAZ KASTELIC is the Lead Cyber Stability Researcher of the Security and Technology Programme at UNIDIR. Prior to joining UNIDIR, he held various research positions at international organizations and research institutions around the world.

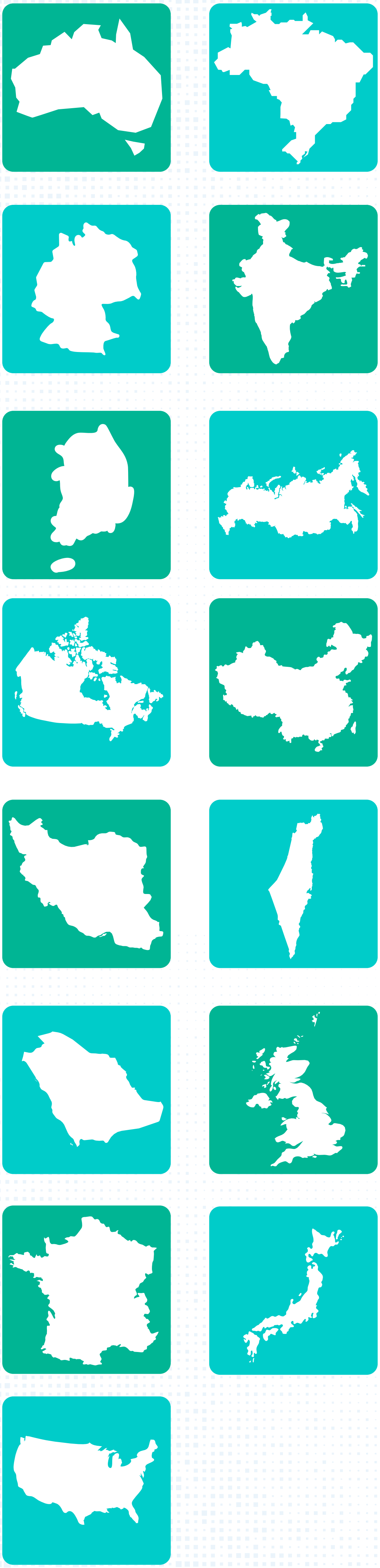

TABLE OF CONTENTS

Introduction

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, for 15 countries across different regions, 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 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.n

Papers part of the series are available at www.unidir.org/cyberdoctrines

Background and Context

Although developments in the field of ICT have endowed society with notable benefits,[1] the use of the underlying technologies for offensive purposes is a widespread and well-publicized issue. Not only are cyber operations used by criminal individuals and organizations for financial gain but, increasingly, **States are using international cyber operations to advance their national agendas in pursuit of strategic interests.**

Over one quarter of United Nations Member States possess such cyber capabilities,[2] and the number of States able to conduct cyber operations in or through foreign connected infrastructure is growing.[3]

According to a think-tank, 33 States have already utilised international cyber operations with the intent to advance their strategic interests in or through foreign ICT infrastructure since 2005.[4]

State conduct of international cyber operations and the development of capabilities to conduct such operations can pose new challenges to international peace and security. International cyber operations may diminish trust between States,[5] and a number of States have expressed concern that the continuous development of national capabilities to conduct such operations undermines international peace and security.[6]

[1] UNCTAD (2020).
[2] Geneva Digital Platform (2020). Some argue the number is in fact significantly higher; see, for example, Smeets (2018, 90).
[3] General Intelligence and Security Service, Netherlands (2020).
[4] Council on Foreign Relations (2020).
[5] UNODA (2018, 56).
[6] For example, NAM (2020).

Concept of International Cyber Operations

This research paper series investigates national capabilities and doctrines related to the international cyber operations conducted, effectively controlled or directed by a State.[7]

For the purpose of this publication, an international cyber operation denotes a proactive use of a State's cyber capabilities to **project its power in or through cyberspace under a foreign jurisdiction.** Accordingly, the focus of the series is not cyber operations in the context of self-defence, as governed by the provisions found in the United Nations Charter, but a proactive use of cyber capabilities to advance the strategic objectives of a State.

The analysis provided by the series of papers focuses on international cyber operations that compromise "the confidentiality, integrity, or availability"[8] of systems and networks under a foreign jurisdiction. As such, the papers analyse capabilities to conduct international cyber operations and relevant national doctrines, regardless of the (intended) consequence of a cyber operation; the papers consider destructive, disruptive and non-destructive cyber operations.

The disruptive or destructive cyber operations considered by the series are often labelled cyberattacks, offensive cyber operations,[9] pre-emptive or anticipatory cyber (self-)defence,[10] persistent cyber engagement,[11] defence forward,[12] out-of-network cyber operations,[13] proactive cyber deterrence[14] or similar.

Given that international cyber operations are not necessarily of a disruptive or destructive nature but can instead result in compromised confidentiality or integrity of the information held by the infrastructure under a foreign jurisdiction, the research paper series also analyses operations characterized by States and scholarship as, for instance, cyber espionage,[15] cyber exploitation[16] or territorially intrusive intelligence collection.[17]

[7] UNGA (2002, annex, arts 4–11).
[8] Lin & Zegart (2017, 1).
[9] For example, Uren et al. (2018).
[10] For example, DeWeese (2015).
[11] For example, United States Cyber Command (2018).
[12] For example, United States Department of Defense (2018).
[13] For example, Smeets (2019).
[14] For example, Libicki (2009).
[15] For example, Centre for the Protection of National Infrastructure (2020).
[16] For example, Lin (2010).
[17] For example, Scott (1999).

International Cyber Operations and Implications for International Peace and Security

International cyber operations, whether disruptive or destructive, or an infringement of the confidentiality or integrity of the information stored on the foreign infrastructure, challenge the stability of international relations and may endanger international peace and security. This is particularly true of international cyber operations outside the context of an international armed conflict, which can be perceived as laying down the grounds for an upcoming large-scale attack or interpreted as a breach of a State's sovereignty.

Given that most large-scale destructive cyber operations are planned well in advance and involve "an initial stage of reconnaissance and intrusion",[18] any **unauthorized intrusion into the networked infrastructure prior to or outside of an armed conflict could be interpreted as a preparatory step towards a digital or kinetic operation.**[19]

Moreover, States could very well interpret any **international cyber operation as a breach of their sovereignty and a foundation for lawful retaliatory reaction, bearing the possibility of escalation.** The applicability of the principle of sovereignty and the resulting legal obligations pertaining to conduct in cyberspace were confirmed by the 2015 report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,[20] subsequently adopted by the United Nations General Assembly.[21]

Although the intricacies of the principle and the emanating international legal obligations have not been agreed on by the international community, some States interpret the unauthorized penetration of networks or systems under foreign jurisdiction as a violation of the principle, or even the rule,[22] of sovereignty. The position of the French government, for example, is that "any unauthorised penetration by a State of French systems or any production of effects on French territory via a digital vector may constitute, at the least, a breach of sovereignty".[23]

Even in the absence of destruction, such actions could attract retaliatory response by a victim State and lead to a spiral of conflict, threatening international peace and security. Instances of *opinio juris* confirm this assertion; for example, when a cyber operation "affects the military or economic power, security or survival capacity of the Nation, or constitutes interference in France's internal or external affairs, [the response of France may] entail defensive cyber warfare operations".[24] Similarly, China announced it will "use whatever means necessary — scientific, technological, legal, diplomatic or military — to ensure cyberspace sovereignty".[25]

Cyber operations against critical systems can attract a response that involves not only cyber capabilities but also physical weapons, as demonstrated in 2019 by Israel responding to a cyber operation by way of an airstrike.[26] Crucially, the Russian Federation and the United States of America, both permanent members of the United Nations Security Council, do not exclude the possibility of nuclear retaliation to a cyber operation,[27] and academics have openly urged China to ready its nuclear arsenal to be able to respond to an international cyber operation intended to paralyse Chinese networks.[28]

[18] Diaz (2018).

[19] Foreign network presence could very well lead to the conclusion that a network has been "infected with hidden software that could be triggered in a crisis to disrupt or destroy data or communications" (Hathaway (2008)).

[20] "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory" (UNGA (2015b)).

[21] UNGA (2015a).

[22] Whether sovereignty constitutes a principle or a rule of the international law remains unsettled. For a brief overview see, for example, Schmitt (2020).

[23] Ministry of Armed Forces, France (2019, 6).

[24] Ministry of Armed Forces, France (2019, 7).

[25] The State Council the People's Republic of China (2016).

[26] Chesney (2019); Gross (2019).

[27] For analysis of the Russian and US positions, see, for example, Klare (2019); Stefanovich (2020).

[28] An (2020); Browne (2013).

Purpose and unique nature of this series of papers

By providing a systematic overview of national frameworks guiding or restraining the use of States' capabilities to conduct international cyber operations, and therefore by elaborating on the ways in which States operate in cyberspace, this series attempts to contribute to transparency and predictability in the behaviour of States. To an extent, the papers of the series thus complement UNIDIR's Cyber Policy Portal,[29] an online repository of national and institutional cyber policy landscapes, promoting information-sharing and confidence-building. Much like the Cyber Policy Portal, the research paper series is one of the research activities of the Cyber Stability workstream, part of UNIDIR's Security and Technology Programme.

The contributions to the series will be appreciated by policymakers, international law professionals, scholars and non-State actors affected by the developments in international cybersecurity. The individual contributions have been drafted by independent academics and practitioners with distinct knowledge of the relevant national doctrines and capabilities. The wealth of their knowledge has been condensed into lucid and digestible overviews of the national capabilities and doctrines.

While studies into the theoretical conceptualization of offensive cyber operations and of cyber operations in a narrow military context exist,[30] at the time of writing there are no comparable comprehensive studies outlining the capabilities or doctrines of the 15 countries analysed by the present series.

The papers will also contribute to the emerging scholarship investigating offensive cyber capabilities and their use. As a collection, the series encourages readers to draw conclusions based on a comparison between different national approaches to international cyber operations.

[29] www.cyberpolicyportal.org

[30] See, for example, IISS (2020, ch. 10); Lin & Zegart (2017); Uren et al. (2018).

Methodology

The paper series focuses on doctrines and capabilities relating to the conduct of international cyber operations by 15 countries selected from the 20 top military spenders in 2018[31] and representing different regions of the world:

- Australia
- Brazil
- Canada
- China
- France
- India
- Iran, Islamic Republic of
- Israel
- Japan
- Korea, Republic of
- Russian Federation
- Saudi Arabia
- United Kingdom of Great Britain and Northern Ireland
- United States of America

As such, the collection of papers provides an analysis of the doctrines and capabilities of countries from all the continents except Africa. The reason for this is that the military expenditures of African States are significantly lower than that of the 20 top military powers; the military expenditures of Morocco, the forty-third State on the list of global military spending and the highest ranking African State,[32] are nearly three times less than the expenditures of the Islamic Republic of Iran, which ranks twentieth, for example.

We set out to analyse the countries with the biggest proportion of global military spending on the assumption that **military spending, at least to a certain degree, translates to spending dedicated to the development of international cyber operation capabilities.** The assumption was necessary owing to the absence of comprehensive and reliable public data on the expenditure of States for international cyber operations.

The sources reviewed by the contributing authors and considered to form a national doctrine on the conduct of international cyber operations include primary sources – such as national guidelines, policies, strategies, regulatory instruments and domestic laws – regulating the deployment of cyber capabilities with the intention of penetrating foreign networks and connected infrastructure, regardless of the specific purpose of such an action. To augment the primary sources, the authors relied on such secondary resources as monographs, journal articles and interviews with local subject matter experts.

[31] Annual defense budget in US dollars (SIPRI (2020)).

[32] The military spending of Algeria is higher than that of Morocco, but the data are "highly uncertain" and thus not considered here. See SIPRI (2020).

Conclusion

International cyber operations have the potential to challenge international peace and security. To facilitate transparency and contribute to the predictability of State behaviour in cyberspace, this unique series of papers analyses the postures of 15 States and offers an overview of their capabilities to conduct international cyber operations as well as their national doctrines guiding the conduct of such operations.

Because of the ever-evolving landscape and the often secretive nature of national offensive cyber programmes, the series does not pretend to be or to indefinitely stay the most comprehensive study of these States' capabilities and doctrines. Aside from outlining the current situation and current national postures, the series aims to spark further research into international cyber operations and relevant national postures. Additional research should be conducted as the landscape changes, as new capabilities are developed and as doctrines are amended or become accessible to the research community.

Future investigations could also be focused on expanding to other States. Because cyber operations qualify as an asymmetric threat, a significant impact on international peace and security could result from actions of a State with a military investment lower than that of the top 20 military spenders analysed by this paper series.

References

An, Qin. 2020. 'Nuclear deterrence needed to prevent cyberattacks from paralyzing China's nuclear response.' *Global Times*, 24 August, 2:42 p.m. As of 8 November 2020: https://www.globaltimes.cn/content/1198665.shtml

Browne, Andrew. 2013. 'China: Cyberattacks Are Like Nuclear Bombs.' *Wall Street Journal*, 22 April, 10:48 p.m. As of 8 November 2020: https://www.wsj.com/articles/SB10001424127887323551004578438842382520654

Centre for the Protection of National Infrastructure. 2020. 'Espionage.' As of 8 November 2020: https://www.cpni.gov.uk/espionage

Chesney, Robert. 2019. 'Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility.' *Lawfare*, 6 May, 2:27 p.m. As of 8 November 2020: https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility

Council on Foreign Relations. 2020. 'Cyber Operations Tracker.' As of 8 November 2020: https://www.cfr.org/cyber-operations/#OurMethodology

DeWeese, Geoffrey. 2015. 'Anticipatory and Preemptive Self-Defence in Cyberspace: The Challenge of Imminence.' In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, edited by M. Maybaum, A.-M. Osula & L. Lindström, 81–92. Tallin: NATO CCD COE Publications.

Diaz, Vicente. 2018. 'Kaspersky Security Bulletin 2018. Threat Predictions for 2019.' SecureList, 20 November, 10:00 a.m. As of 8 November 2020: https://securelist.com/kaspersky-security-bulletin-threat-predictions-for-2019/88878

General Intelligence and Security Service, Netherlands. 2020. 'Offensive Cyber-Programmes: An Ideal Business Model for States.' February. As of 30 October: https://english.aivd.nl/publications/publications/2020/02/26/publication-aivd-offensive-cyber-programmes---an-ideal-business-model-for-states

Geneva Digital Platform. 2020. 'UN GGE and OEWG.' As of 8 November 2020: https://dig.watch/processes/un-gge#view-7541-2

Gross, Judah Ari. 2019. 'IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle.' *Times of Israel*, 5 May. As of 16 March 2021: https://www.timesofisrael.com/liveblog_entry/idf-says-it-thwarted-hamas-cyber-attack-amid-rocket-attacks

Hathaway, Melissa. 2008. 'Cyber Security: An Economic and National Security Crisis.' *The Intelligencer: Journal of U.S. Intelligence Studies* 16 (2): 31–36.

International Institute for Strategic Studies (IISS). 2020. *The Military Balance 2020*. Abingdon: Routledge.

Klare, Michael. 2019. 'Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation.' *Arms Control Today*, 49 (9): 6–13.

Libicki, Martin. 2009. 'Cyberdeterrence and Cyberwar.' RAND Corporation. As of 8 November 2020: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Lin, Herbert. 2010. 'Offensive Cyber Operations and the Use of Force.' *Journal of National Security Law & Policy* 4: 63–86.

Lin, Herbert, & Amy Zegart. 2017. 'Introduction to the Special Issue on Strategic Dimensions of Offensive Cyber Operations.' *Journal of Cybersecurity* 3 (1): 1.

Ministry of Armed Forces, France. 2019. 'International Law Applied to Operations in Cyberspace.' As of 8 November 2020: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf

Non-Aligned Movement (NAM). 2020. 'NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG).' As of 4 February 2020: https://front.un-arm.org/wp-content/uploads/2020/04/nam-wp-to-the-oewg-final.pdf.

Schmitt, Michael N. 2020. Sovereignty, Intervention, and Autonomous Cyber Capabilities. *International Law Studies* 96: 549–576

Scott, Roger. 1999. 'Territorially Intrusive Intelligence Collection and International Law.' *Air Force Law Review* 46: 217–26.

Smeets, Max. 2018. 'The Strategic Promise of Offensive Cyber Operations.' *Strategic Studies Quarterly* 12 (3): 90–113.

———. 2019. 'NATO Allies Need to Come to Terms with Offensive Cyber Operations.' *Lawfare*, 14 October, 8:08 a.m. As of 8 November 2020: https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations

State Council the People's Republic of China. 2016. 'China announces cybersecurity strategy.' 27 December. As of 13 April 2021: http://english.www.gov.cn/state_council/ministries/2016/12/27/content_281475526667672.htm

Stefanovich, Dmitry. 2020. 'Russia's Basic Principles and the Cyber-Nuclear Nexus.' European Leadership Network, 14 July. As of 8 November 2020: https://www.europeanleadershipnetwork.org/commentary/russias-basic-principles-and-the-cyber-nuclear-nexus

Stockholm International Peace Research Institute (SIPRI). 2020. 'Military Expenditure Database.' As of 8 November 2020: https://www.sipri.org/databases/milex

United Nations Conference on Trade and Development (UNCTAD). 2020. 'ICT Offers Great Potential for Development, but also Risks.' SDG Pulse. As of 8 November 2020: https://sdgpulse.unctad.org/ict-development

United Nations General Assembly (UNGA). 2002. Responsibility of States for internationally wrongful acts, UN Document A/RES/56/83, 28 January 2002.

———. 2015a. *Developments in the field of information and telecommunications in the context of international security*, UN Document A/RES/70/237, 30 December 2015.

———. 2015b. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Document A/70/174, 22 July 2015.

United Nations Office for Disarmament Affairs (UNODA). 2018. *Securing Our Common Future: An Agenda for Disarmament*. New York. As of 8 November 2020: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf

United States Cyber Command. 2018. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. As of 8 November 2020: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf

United States Department of Defence. 2018. 'Summary: Department of Defence Cyber Strategy 2018.' As of 8 November 2020: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Uren, Tom, Bart Hogeveen & Fergus Hanson. 2018. 'Defining offensive cyber capabilities.' 4 July. As of 18 February 2021: https://www.aspi.org.au/report/defining-offensive-cyber-capabilities

International Cyber Operations:
National Doctrines and Capabilities

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.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH